2020-12

CYBERCRIME RESPONSE CAPABILITIES AND CAPACITY: AN EVALUATION OF LOCAL LAW ENFORCEMENTS RESPONSE TO A COMPLEX PROBLEM

Monaghan, Ryan M.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CYBERCRIME RESPONSE CAPABILITIES AND CAPACITY: AN EVALUATION OF LOCAL LAW ENFORCEMENT'S RESPONSE TO A COMPLEX PROBLEM

by

Ryan M. Monaghan

December 2020

Co-Advisors: Robert L. Simeral (contractor)
Nadav Morag (contractor)

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2020	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
CYBERCRIME RESPONSE CAPABILITIES AND CAPACITY: AN EVALUATION OF LOCAL LAW ENFORCEMENT'S RESPONSE TO A COMPLEX PROBLEM

5. FUNDING NUMBERS

6. AUTHOR(S) Ryan M. Monaghan

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Local law enforcement is expected to respond to cybercrimes by having the appropriate level of capabilities and capacity for highly technical and complex investigative activities. Having the specialized resources necessary to have this type of investigative capabilities and capacity presents significant challenges for local law enforcement agencies regardless of size. Small and midsize agencies face even greater challenges based on a lack of necessary resources, ranging from trained personnel to funding. Adding to the list challenges is a lack of standardization, policies, and protocols to provide guidance to agencies looking for strategies to address the need for cybercrime investigative capabilities and capacity. This thesis examined different models being used by local law enforcement agencies of all sizes to address the need for cybercrime investigative capabilities and capacity and lumped them into three models: internal resources, conventional task forces, and hybrid task forces. Using strengths, weaknesses, opportunities, threats (SWOT) analysis, the three models were examined. The findings revealed commonalities and differences between the models, highlighting potential pros and cons for each. Recommendations were made for local law enforcement decision makers to consider when developing policies and protocols around their need for cybercrime investigative capabilities and capacity.

14. SUBJECT TERMS cybercrime, cybercrime investigative capabilities and capacity, local law enforcement, conventional task force, hybrid task force, internal resources	**15. NUMBER OF PAGES** 111
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

CYBERCRIME RESPONSE CAPABILITIES AND CAPACITY: AN EVALUATION OF LOCAL LAW ENFORCEMENT'S RESPONSE TO A COMPLEX PROBLEM

Ryan M. Monaghan
Lieutenant, San Mateo Police Department
BS, Union Institute & University, 2017

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2020**

Approved by: Robert L. Simeral
Co-Advisor

Nadav Morag
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Local law enforcement is expected to respond to cybercrimes by having the appropriate level of capabilities and capacity for highly technical and complex investigative activities. Having the specialized resources necessary to have this type of investigative capability and capacity presents significant challenges for local law enforcement agencies regardless of size. Small and midsize agencies face even greater challenges based on a lack of necessary resources, ranging from trained personnel to funding. Adding to the list challenges is a lack of standardization, policies, and protocols to provide guidance to agencies looking for strategies to address the need for cybercrime investigative capabilities and capacity. This thesis examined different models being used by local law enforcement agencies of all sizes to address the need for cybercrime investigative capabilities and capacity and lumped them into three models: internal resources, conventional task forces, and hybrid task forces. Using strengths, weaknesses, opportunities, threats (SWOT) analysis, the three models were examined. The findings revealed commonalities and differences between the models, highlighting potential pros and cons for each. Recommendations were made for local law enforcement decision makers to consider when developing policies and protocols around their need for cybercrime investigative capabilities and capacity.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

BJA	Bureau of Justice Assistance
BJS	Bureau of Justice Statistics
CATCH	Computer and Technology Crime High Tech Response Team
CDFU	Computer and Digital Forensic Unit
CHDS	Center for Homeland Defense and Security
CTF	Cyber Task Force
DHS	Department of Homeland Security
DTS	Department of Technology Services
ECTF	Electronic Crimes Task Force
FBI	Federal Bureau of Investigation
HTTAP	High Technology Theft Apprehension and Prosecution
IC3	Internet Crime Complaint Center
ICAC	Internet Crimes against Children Task Force
IMPD	Indianapolis Metropolitan Police Department
LEMAS	Law Enforcement Management and Administrative Statistics
MCDABI	Monterey County, California District Attorney's Office Bureau of Investigation
MNPD	Metropolitan Nashville Police Department
NC3TF	Northern California Computer Crimes Task Force
NCFI	National Computer Forensic Institute
NIBRS	National Incident-Based Reporting System
OWS	Operation Wellspring
PERF	Police Executive Research Forum
RCFL	Regional Computer Forensics Laboratories
REACT	Regional Enforcement Allied Computer Team
SBI	Utah Department of Public Safety's State Bureau of Investigation
SCCSO	Santa Clara County Sheriff's Office
SCHTTF	Southern California High Tech Task Force
SIAC	Statewide Information and Analysis Center
SIM	subscriber identity module

SVHCTF	Sacramento Valley Hi-Tech Crimes Task Force
SWOT	strengths, weaknesses, opportunities, threats
UCCTF	Utah Cyber Crimes Task Force
UCR	Uniformed Crime Reporting Program
UDPS	Utah Department of Public Safety

EXECUTIVE SUMMARY

The over 18,000 U.S. local law enforcement agencies are expected to enforce laws and investigate crimes; cybercrime is no exception. According to data from the Internet Crime Complaint Center (IC3), which only accounts for some of the reported cybercrimes, cybercrimes continue to proliferate. As indicated in the first page of the *U.S. Department of Homeland Security Cybersecurity Strategy*, securing this nation's cyberspace is a homeland security responsibility shared between local, state, and federal law enforcement agencies. It is not just about the prevention of crimes in cyberspace; it also includes disrupting cybercrime and holding cybercriminals accountable. Contrary to the popular belief that investigating cybercrimes is only the responsibility of federal law enforcement agencies, local enforcement agencies are on the frontlines of the fight against cybercrime.[1] With the majority of local law enforcement agencies in the United States being small in size, and having limited cybercrime investigative capabilities, cybercrime-related enforcement efforts can be a daunting task.[2] Regardless of the challenges, local law enforcement must have the ability to deal with cybercrime.

The challenges associated with cybercrime investigative activities for local law enforcement agencies run the gamut. No national standard for expectations exists on the level of cybercrime capabilities and capacity local law enforcement agencies should have and a lack of policies and protocols to guide the response to and training in cybercrime-related topics.[3] Local law enforcement agencies' current strategies for addressing

---

[1] Chuck Wexler, *The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime* (Washington, DC: Police Executive Research Forum, 2014), 2, https://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf; Thomas J. Holt and Adam M. Bossler, "Predictors of Patrol Officer Interest in Cybercrime Training and Investigation in Selected United States Police Departments," *Cyberpsychology, Behavior, and Social Networking* 15, no. 9 (December 2012): 464–465, https://doi.org/10.1089/cyber.2011.0625.

[2] Todd G. Shipley and Art Bowker, "Introduction to Internet Crime," in *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, ed. Nick Selby (Waltham, MA: Elsevier Science & Technology Books, 2013), 12–13, ProQuest.

[3] Shipley and Bowker, 13; Chuck Wexler, *New National Commitment Required: The Changing Nature of Crime and Criminal Investigations* (Washington, DC: Police Executive Research Forum, 2018), 8.

cybercrime is another challenge that they face. It is hard for decision makers to make an informed decision because studies that may otherwise provide valuable data on the different types of strategies or models used to address cybercrime investigative capabilities and capacity are lacking.

This thesis set out to help close the gap in research related to the different cybercrime response strategies or models by answering the research question. Of three common models local law enforcement agencies employ to address cybercrime investigative capabilities and capacity—internal resources, conventional task forces, and hybrid task forces—is one or a combination thereof best suited to address the needs of small, midsize, or large agencies? To answer this question, the SWOT, which is an acronym for strengths, weaknesses, opportunities, and threats, analysis framework was used for analysis of the three different models. SWOT analysis was chosen because of its longstanding history of usage for examining internal and external factors that influence organizational environments.[4] The analysis focused on three key attributes of each of three models that had the most significant influence over cybercrime investigative capabilities and capacity: level of cybercrime-investigative training and expertise development for personnel, prioritization of cybercrime-related cases, and funding sources.

The results of the SWOT analysis were: (1) a qualitative assessment of the three different models described in the study, (2) recommendations for local law enforcement decision makers to consider when developing policies and protocols to address cybercrime investigative capabilities and capacity, and (3) recommendations for future research.

The findings of the SWOT analysis revealed commonalities and differences between the internal resources, conventional task forces, and hybrid task forces models. The commonalities were opportunities for cybercrime investigative training among first responders and other personnel not serving in cybercrime investigative roles for all three

[4] David W. Pickton and Sheila Wright, "What's SWOT in Strategic Analysis?," *Strategic Change* 7, no. 2 (1998): 102–3, https://doi.org/10.1002/(SICI)1099-1697(199803/04)7:2%3C101::AID-JSC332%3E3.0.CO;2-6; Marilyn M. Helms and Judy Nixon, "Exploring SWOT Analysis—Where Are We Now? A Review of Academic Research from the Last Decade," *Journal of Strategy and Management* 3, no. 3 (2010): 215–18, https://doi.org/10.1108/17554251011064837.

models, threats related to funding for all three models, and strengths related to case prioritization for the internal resources and hybrid task forces models. The differences were weaknesses related to workload capacity with the internal resources model, weaknesses related to case prioritization with the conventional task forces model, and weaknesses related to decentralized makeup of the hybrid task forces model.

The recommendations were grouped by their relevance to different size local law enforcement agencies. As defined in this study, small agencies were those with fewer than 60 officers or serving populations of fewer than 60,000, midsize agencies were those with between 60 and 99 officers or serving populations between 60,000 to 99,000, and large agencies were those with over 99 officers or serving populations over 99,000. For small to midsize agencies, the recommendations were participation in the hybrid task forces models and consolidation and sharing of internal cybercrime resources. For large agencies, the recommendation was for combining internal resources with the conventional or hybrid task forces models. For small, midsize, and large agencies, the recommendation was training to increase cybercrime capabilities for all agency personnel.

The thesis concluded by answering the research question that established the foundation for the study. In doing so, an argument was made for the hybrid task forces models as being the most adaptable to fit the needs of small, midsize, and large local law enforcement agencies alike with a caution that it is not a “one size fits all solution” based on the findings of the study. Future research recommendations are made for studying the effectiveness of each model that includes both qualitative and quantitative data, what an effective distribution of cybercrime investigative knowhow throughout local law enforcement agencies would entail, and the level of cybercrime investigative training that should be provided to new and experienced officers.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I dedicate this thesis to my father, Michael J. Monaghan, who unexpectedly passed away just prior to me completing this program. My father instilled in me a strong sense of perseverance and mental fortitude. He was very proud of my chosen career path and with my decision to pursue my master's degree at the Naval Postgraduate School. Although not physically present on graduation day, I know he was there. I did it, Dad!

I need to thank many people for my success in this endeavor. I would be remiss to not recognize retired San Mateo Police Chief Susan Manheimer for allowing me to take part in this incredible journey. I would also like to thank San Mateo County Manager and retired San Mateo Police Deputy Chief, Mike Callagy, for sharing with me the sense of pride he had as a Center for Homeland Defense and Security (CHDS) alumni and for his encouragement, advice, and assistance along the way. In addition to Mike, other San Mateo County CHDS alumni assisted me with letters of recommendation, encouragement, and advice. I will do my part by paying it forward.

I am also indebted to my advisors and the amazing staff of CHDS. You all do the extraordinary to support all of us students. You have challenged me to examine problems through a different lens and to be a better homeland security leader. National Capital Region Cohort 1803/1804, I am thankful to have shared this journey with all of you. I consider you all friends for life no matter how much time and distance separates us.

Last, but certainly not least, I am forever grateful to my family and friends who supported me along the way. To my mom, Helen, and my stepdad, Ed, thank you for always believing in me. To my sister, Dana, and my brother, Michael, thank you for your unwavering support. To my large extended family and friends, too many to name, thank you for enriching my life. To my love, Amy, thank you for supporting my wild endeavors and for keeping our family in order so I could immerse myself into this program. I could never thank you enough. Your love and support mean the world to me. To my amazing daughter, Hannah, thank you for being so patient while I was away and busy. I hope my journey inspires you to never stop learning and go after all the great things the world has to offer you. As proud as I am of this accomplishment, nothing makes me prouder than being your dad.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The over 18,000 U.S. local law enforcement agencies are expected to enforce laws and investigate crimes; cybercrime is no exception. As indicated in the first page of the *U.S. Department of Homeland Security Cybersecurity Strategy*, securing this nation's cyberspace is a homeland security responsibility shared between local, state, and federal law enforcement agencies. It is not just about the prevention of crimes in cyberspace; it also includes disrupting cybercrime and holding cybercriminals accountable. Contrary to the popular belief that investigating cybercrimes is only the responsibility of federal law enforcement agencies, local enforcement agencies are on the frontlines of the fight against cybercrime.[1] With the majority of local law enforcement agencies in the United States being small in size, and having limited cybercrime investigative capabilities, cybercrime-related enforcement efforts can be a daunting task.[2] Despite resources and other challenges, local law enforcement agencies, regardless of size, must have the capabilities and capacity for cybercrime investigative functions.

Although no one agreed upon definition for cybercrime takes precedence in the law enforcement community, most definitions resemble one another and account for the different types of cybercrimes. For the purposes of this study, Shipley's and Bowker's definition of cybercrime is used: crimes made possible by the emergence of technology, whether they be traditional crimes transformed by technology or crimes facilitated via technology.[3] The most common cybercrimes being reported are thefts that involve non-payment for services or goods received and non-delivery of paid goods and services,

---

[1] Chuck Wexler, *The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime* (Washington, DC: Police Executive Research Forum, 2014), 2, https://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf; Thomas J. Holt and Adam M. Bossler, "Predictors of Patrol Officer Interest in Cybercrime Training and Investigation in Selected United States Police Departments," *Cyberpsychology, Behavior, and Social Networking* 15, no. 9 (December 2012): 15, https://doi.org/10.1089/cyber.2011.0625.

[2] Todd G. Shipley and Art Bowker, "Introduction to Internet Crime," in *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, ed. Nick Selby (Waltham, MA: Elsevier Science & Technology Books, 2013), 12–13, ProQuest.

[3] Shipley and Bowker, 2.

extortion, and breaches of personal data.[4] Cybercrime encompasses a broad spectrum of crimes that affect people everywhere.

Using open-source information from scholarly documents, government reports, and books, supplemented by answers from questionnaires distributed to a cross-section of local law enforcement agencies of varying sizes and multijurisdictional cybercrime task forces, this thesis lumped common strategies for addressing the complex challenges associated with cybercrime investigative capabilities and capacity into three models: internal resources, conventional task forces, and hybrid task forces. The models were examined using a recognized analysis framework. The findings of the analysis set the basis for recommendations regarding policy and protocol considerations for local law enforcement agencies seeking to increase their cybercrime investigative capabilities and capacity.

A. PROBLEM STATEMENT

Cybercrime compromises the security of cyberspace, making it both a homeland security and societal issue. The U.S. economy suffers billions of dollars in loss annually as the result of cybercrime.[5] Reports from the Federal Bureau of Investigation's (FBI's) Internet Crime Complaint Center (IC3) and the Symantec Corporation provide statistical evidence that cybercrime is proliferating. Of the 246 million internet users in the United States, 143 million—or 58 percent—experienced cybercrime in 2017.[6] Data collected between 2013 and 2017 revealed a steady increase in reported instances of internet crimes.[7] Moreover, an excess of 20 billion electronic communication devices will likely be

---

[4] Internet Crimes Complaint Center, *2018 Internet Crime Report* (Washington, DC: Federal Bureau of Investigation, 2018), 19, https://pdf.ic3.gov/2018_IC3Report.pdf.

[5] Kristin Finklea and Catherine A. Theohary, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*, CRS Report No. R42547 (Washington, DC: Congressional Research Service, 2015), 8, https://www.hsdl.org/?view&did=762027.

[6] Symantec Corporation, *2017 Norton Cyber Security Insights Report Global Results* (Mountain View, CA: Symantec Corporation, 2017), 11, https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf.

[7] Internet Crimes Complaint Center, *2017 Internet Crime Report* (Washington, DC: Federal Bureau of Investigation, 2017), 4, https://pdf.ic3.gov/2017_IC3Report.pdf.

connected to the internet by 2020.[8] Digital connectivity has permeated almost every aspect of our daily lives, which thus creates more opportunities for cybercriminals and increasing the demand for local law enforcement to intervene.

The challenges cybercrime investigative tasks create for local law enforcement agencies differ from those associated with traditional or "real-world crimes," and must be addressed differently. Employing traditional data-driven crime mitigation strategies is not effective with cybercrime because of underreporting and current flaws in data collection that yield an incomplete picture of the problem scope.[9] In addition to the data challenges, the level of cybercrime training for local law enforcement is not mandated or standardized.[10] Moreover, no set national standards or any type of unified plan is available for law enforcement's response to cybercrime.[11] Most American local law enforcement agencies lack the resources necessary for the level of investigative capabilities and capacity to perform cybercrime-related functions at a pace that keeps up with the demand.[12] In a 2014 Police Executive Research Forum (PERF) study, local law enforcement agencies from around the nation were queried about the three most significant challenges impeding their ability to perform cybercrime investigations effectively. Of the responding agencies, 54 percent reported a lack of staffing, 31 percent reported a lack of funding, and 29 percent reported a lack of internal expertise.[13] These realities combined with cybercrime's rapidly evolving nature have most law enforcement agencies consistently "behind the curve" in the fight against it. Local law enforcement agencies continue to struggle with effective

---

[8] Department of Homeland Security, *U.S. Department of Homeland Security Cybersecurity Strategy* (Washington, DC: Department of Homeland Security, 2018), 2, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

[9] Finklea and Theohary, *Cybercrime: Conceptual Issues*, 18.

[10] Hollis Stambaugh et al., *Electronic Crime Needs Assessment for State and Local Law Enforcement*, NCJ 186276 (Washington, DC: Department of Justice, Office of Justice Programs, 2001); Brian A. Reaves, *State and Local Law Enforcement Training Academies, 2013*, NCJ 249784 (Washington, DC: Bureau of Justice Statistics, 2013), 5, https://www.bjs.gov/content/pub/pdf/slleta13.pdf.

[11] Shipley and Bowker, "Introduction to Internet Crime," 13.

[12] Mieke Eoyang et al., *To Catch A Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors* (Washington, DC: Third Way, 2018), 14, https://thirdway.imgix.net/pdfs/override/To_Catch_A_Hacker_Report.pdf.

[13] Wexler, *The Role of Local Law Enforcement*, 7.

strategies or models to address all the challenges associated with the investigations of this prevalent crime.[14] The mitigation challenges associated with cybercrimes are likely to remain a constant threat that forces local law enforcement agencies to assess and adapt strategies continually for countering them.

The ways in which local law enforcement agencies currently address cybercrime investigations depend on multiple variables. The most significant variables are related to agency size and the amount of available resources.[15] Some agencies, mostly larger ones, have internal resources to justify dedicated cybercrime units or dedicated specialized personnel, while others have designated personnel capable of performing cybercrime investigative functions. In recent years, the number of midsize to large local law enforcement agencies with dedicated cybercrime units or specialized personnel dedicated to cyber-investigative function has increased.[16] Smaller agencies, with limited resources, often need to rely on partnerships with other agencies or outside resources to help them with complex cybercrime investigative functions.[17] To compensate for the challenges associated with cybercrime investigations, some local law enforcement agencies participate in collaborative cybercrime efforts, such as multijurisdictional task forces models. Task forces combine resources from multiple jurisdictions in an effort to increase the investigative capabilities and capacity of the participating agencies.[18] Some of these task forces include formal and informal agreements from private-sector and academic

---

[14] Sean E. Goodison, Robert C. Davis, and Brian A. Jackson, *Digital Evidence and the U.S. Criminal Justice System* (Santa Monica, CA: RAND, 2015), 6, https://www.rand.org/pubs/research_reports/RR890.html.

[15] Dale Willits and Jeffrey Nowacki, "The Use of Specialized Cybercrime Policing Units: An Organizational Analysis," *Criminal Justice Studies* 29, no. 2 (June 2016): 24, https://doi.org/10.1080/1478601X.2016.1170282.

[16] Brian A. Reaves, *Local Police Departments, 2013: Personnel, Policies, and Practices*, NCJ 248677 (Washington, DC: Bureau of Justice Statistics, 2015), 10, https://www.bjs.gov/content/pub/pdf/lpd13ppp.pdf; Shelley S. Hyland and Elizabeth Davis, *Local Police Departments, 2016: Personnel*, NCJ 252835 (Washington, DC: Bureau of Justice Statistics, 2019), 10, www.bjs.gov/content/pub/pdf/lpd16p.pdf.

[17] Willits and Nowacki, "The Use of Specialized Cybercrime Policing Units," 12.

[18] David Povero, "Municipal Police Agencies Dial 911 When It Comes to Investigating Cyber-Related Crimes in the Future?," *Journal of California Law Enforcement* 49, no. 3 (2015): 17, ProQuest.

subject matter expertise.[19] These varied approaches demonstrate how different factors, such as available resources, drive the agency's ability to address cybercrime investigative functions.

A lack of consensus exists on a strategy or model that local law enforcement agencies of varying sizes can employ to offset the challenges associated with having cybercrime capabilities and capacity. As with the lack of accurate cybercrime statistics, data on the effectiveness of internal cybercrime resources and multijurisdictional efforts is also lacking.[20] Despite many expert opinions about what strategies work the best, little comprehensive analysis or assessment of the common strategies used or touted as being effective have been documented. This gap leaves local law enforcement decision makers at a loss for making an informed decision regarding an effective strategy or model to address their organizations' cybercrime investigative capabilities and capacity.

B. RESEARCH QUESTION

Of three common models local law enforcement agencies employ to address cybercrime investigative capabilities and capacity—internal resources, conventional task forces, and hybrid task forces—is one or a combination thereof best suited to address the needs of small, midsize, or large agencies?

C. LITERATURE REVIEW

The purpose of this literature review is to identify, analyze, and assess available government documents, books, and scholarly sources related to the cybercrime investigative capabilities of local law enforcement agencies. The existing literature provides insight into the body of knowledge on the different approaches local law enforcement agencies use to address challenges with conducting cybercrime and cyber-related investigations. The examination of these sources provides the foundation for

---

[19] Diana S. Dolliver, Carson Collins, and Beau Sams, "Hybrid Approaches to Digital Forensic Investigations: A Comparative Analysis in an Institutional Context," *Digital Investigation* 23 (December 2017): 124, https://doi.org/10.1016/j.diin.2017.10.005.

[20] Wexler, *New National Commitment Required*, 14; William Rhodes et al., *Evaluation of the Multijurisdictional Task Forces (MJTFs), Phase II: MJTF Performance Monitoring Guide*, NCJ 228942 (Cambridge, MA: Abt Associates Inc., 2009), 1, https://www.ncjrs.gov/pdffiles1/nij/grants/228942.pdf.

understanding and analysis of the three common models—internal resources, conventional task forces, and hybrid task forces—local law enforcement agencies employ to address the need for cybercrime investigative capabilities and capacity as defined and described in this study. The literature comes from multiple sources with differing perspectives on a variety of related topics for a more comprehensive study.

1. Internal Resources Model

The literature related to the topic of law enforcement agencies that use the internal resources model, as defined in this study, for cybercrime investigative capabilities and capacity was limited despite the prevalence of these types of resources in larger law enforcement agencies throughout urban areas around the nation. Most of the literature with a nexus to subject matter focused on challenges local law enforcement agencies faced when trying to implement or maintain cybercrime investigative capabilities and capacity.

PERF produced two bodies of work that describe the challenges local law enforcement agencies face with cybercrime investigations and the ways in which agencies are increasing their cybercrime investigative capabilities and capacity. PERF assembled experts in criminal investigations, technology, and police operations and management to inform content in both of their studies.[21] PERF called for local agencies to become involved in the fight against criminals harnessing technology and the internet by the creation of a workforce, supported by policies and protocols, capable of performing cybercrime investigative functions.[22] Based on mostly anecdotal evidence from subject matter experts, PERF advocates for agencies to find employees within their organizations who possess the technical skills to serve in specialized cybercrime investigative roles.[23] Additionally, the experts argue for recruiting personnel who already have the technical competency and for civilianizing certain cybercrime investigative roles to increase the pool of qualified applicants.[24] PERF's subject matter experts contend that local law

---

[21] Wexler, *New National Commitment Required*, 1; Wexler, *The Role of Local Law Enforcement*, 1–2.

[22] Wexler, *New National Commitment Required*, 8.

[23] Wexler, *The Role of Local Law Enforcement*, 27–28.

[24] Wexler, *New National Commitment Required*, 55–56.

enforcement agencies can build their cybercrime investigative capabilities and capacity by spreading basic cybercrime investigative knowhow throughout the organization from patrol officers, who are the first link in the investigative process, to detectives.[25] PERF cites multiple agencies for successfully incorporating cybercrime investigative capabilities and capacity throughout their agencies by reimaging traditional operational and organizational structures that incorporate digital investigation experts.[26] The works from PERF rely mostly on anecdotal data from local law enforcement practitioners and decision makers.

Scholarly and government-sponsored studies provide arguments for local law enforcement agencies having their own internal cybercrime investigative resources, as well as explanations for how jurisdictional and departmental factors influence their existence. A 2016 study by Willits and Nowacki titled "The Use of Specialized Cybercrime Policing Units: An Organizational Analysis," contended that agency size, type, level of specialization, and available resources dictates whether or not a local law enforcement agency will have a dedicated cybercrime unit.[27] Willits and Nowacki build upon their assertions from their 2016 study in a 2019 study titled "An Organizational Approach to Understanding Police Response to Cybercrime," and contend that large agencies have more of a jurisdictional need to have their own specialized cybercrime units.[28] According to a study by Bandl, the most significant factor linked to the level of specialization in a local law enforcement agency is the size of the agency.[29] In their 2016 study, Willits and Nowacki asserted that as internal cybercrime units proliferated, smaller jurisdictions without a legitimate need for such a unit were more likely to form one based on decision

---

[25] Wexler, 60–61; Wexler, *The Role of Local Law Enforcement*, 32.

[26] Wexler, *New National Commitment Required*, 54.

[27] Willits and Nowacki, "The Use of Specialized Cybercrime Policing Units," 30.

[28] Jeffrey Nowacki and Dale Willits, "An Organizational Approach to Understanding Police Response to Cybercrime," *Policing: An International Journal* 43, no. 1 (November 2019): 71, https://doi.org/10.1108/PIJPSM-07-2019-0117.

[29] Steven G. Bandl, "The Characteristics and Structure of Police Organizations," in *Police in America* (Thousand Oaks, CA: SAGE Publications, Inc., 2018), 46.

makers feeling pressure from stakeholders.[30] Harkin, Whelan, and Chang argue that cybercrime units have "proliferated" and are becoming the norm in today's police organizations.[31] The findings in the studies published by Willits and Nowacki, as well as Harkin, Whelan, and Chang are confirmed in a comparison of the data presented in Bureau of Justice Statistics (BJS) studies published in 2015 and 2019. These studies revealed that agencies employing 100 or more officers or serving populations of 100,000 or more had a 19.3 percent increase between 2003 and 2016 in personnel designated for cybercrime investigative functions of which 21.2 percent accounted for personnel assigned to specialized cybercrime units.[32] Despite multiple published studies explaining some of the drivers behind why more law enforcement agencies have designated internal resources for cybercrime investigative functions, original empirical research in this area is still relatively limited.[33] The available literature provides evidence that local law enforcement agencies have become more invested in having their own cybercrime capabilities and capacity by designating more internal resources for cybercrime investigative functions.

Although scholarly research and government studies provide explanations for why local law agencies are designating personnel or entire units for cybercrime investigative activities, research into the advantages and disadvantages of maintaining these types of internal resources or any comparative data with other available models that leverage outside resources is lacking. A comparison between data from BJS studies conducted in 2013 and 2016 revealed a 7.1 percent decrease in staff designated for cybercrime investigative functions in local law enforcement agencies employing less than 100 officers or serving populations of less than 100,000 residents.[34] The explanation for the decrease is not explained in the study and raises important questions as to the reasons for the

---

[30] Willits and Nowacki, "The Use of Specialized Cybercrime Policing Units," 10.

[31] Diarmaid Harkin, Chad Whelan, and Lennon Chang, "The Challenges Facing Specialist Police Cyber-Crime Units: An Empirical Analysis," *Police Practice and Research* 19, no. 6 (November 2018): 519–20, https://doi.org/10.1080/15614263.2018.1507889.

[32] Reaves, *Local Police Departments, 2013*, 10; Hyland and Davis, *Local Police Departments, 2016*, 10.

[33] Harkin, Whelan, and Chang, "The Challenges Facing Specialist Police Cyber-Crime Units," 520.

[34] Reaves, *Local Police Departments, 2013*, 9; Hyland and Davis, *Local Police Departments, 2016*, 10.

decrease. More recent studies conducted by Harkin, Whelan, and Chang and PERF provided empirical and anecdotal evidence of workload capacity challenges for personnel who perform cybercrime functions within local law enforcement agencies but lacked research on alternative approaches for reducing the workload.[35] The existing literature related to local law enforcement agencies with internal resources for cybercrime investigative capabilities and capacity provided multiple arguments for having such resources but was not comprehensive enough to explain the pros and cons of the model related to other available models or strategies.

2. Conventional Task Forces Model

The literature related to the conventional task forces model, as defined in this study, was limited and underdeveloped compared to the literature available on the general topic of cybercrime. The conventional task forces model involves participating agencies providing personnel who, in turn, work under the task forces chain-of-command and from a centralized location. One of the main reasons for the formation of conventional task forces was to deal with the demands associated with cybercrime investigations that often exceed the capabilities and capacity of a single law enforcement agency.[36] Both a 2001 study conducted by the National Institute of Justice and a more recent study by PERF provide arguments for why participation in regionalized cybercrime task forces is an effective strategy for local law enforcement agencies to increase their cybercrime investigative capabilities and capacity.[37] Subject matter experts contend cybercrime investigations are a "team sport" that do not occur in a vacuum, which thus makes them highly compatible with multijurisdictional collaborative efforts, such as the conventional

---

[35] Harkin, Whelan, and Chang, "The Challenges Facing Specialist Police Cyber-Crime Units," 523–24; Police Executive Research Forum, *The Utah Model: A Path Forward for Investigating and Building Resilience to Cyber Crime* (Washington, DC: Bureau of Justice Assistance, 2017), 27, http://www.iacpcybercenter.org/wp-content/uploads/2015/04/The-Utah-Model-A-Path-Forward-for-Investigating-and-Building-Resilience-to-Cybercrime.pdf.

[36] Willits and Nowacki, "The Use of Specialized Cybercrime Policing Units," 10.

[37] Stambaugh et al., *Electronic Crime Needs Assessment,* 33; Police Executive Research Forum, *The Role of Local Law Enforcement,* 18.

task forces model.[38] Scholarly studies and subject matter experts contend that cybercrime-related investigations require multijurisdictional collaboration because of their cross-jurisdictional nature and the volume of cases creating investigative capacity challenges for one agency.[39] In a 2010 thesis by Michael P. Callagy, multiple arguments were made for consolidated policing efforts over efforts from individual police agencies.[40] In a 2018 report by PERF, subject matter experts asserted that cybercrime investigative capabilities and capacity challenges were addressed more efficiently when local and state law enforcement agencies combine specialized resources (personnel and equipment) in regionalized efforts.[41] The complex multijurisdictional nature of cybercrimes lends itself to the conventional task forces model.

Despite conventional crime task forces being in existence for decades, research on them is limited, which makes answers to questions regarding their effectiveness unclear. With no agreement on performance metrics for measuring the success of multijurisdictional task forces, data regarding their effectiveness is lacking.[42] Since the early 1980s, conventional task forces have been used for combatting narcotics-related and other high-profile crimes. The 2013 BJS Law Enforcement Management and Administrative Statistics (LEMAS) data that revealed 49 percent of all local law enforcement agencies' narcotics task forces provides evidence of their continued popularity.[43] Two separate studies, one from 1998 and the other from 2000, resulted in a lack of conclusive evidence supporting

---

[38] Wexler, *The Role of Local Law Enforcement*, 18.

[39] Peter Bednar, Vasilios Katos, and Cheryl Hennell, "The Complexity of Collaborative Cyber Crime Investigations," *Digital Evidence and Electronic Signature Law Review* 6 (2009): 214, https://doi.org/10.14296/deeslr.v6i0.1894.

[40] Michael P. Callagy, "Can Local Police and Sheriff's Departments Provide a Higher Degree of Homeland Security Coordination and Collaboration through Consolidation of Police Services?" (master's thesis, Naval Postgraduate School, 2010), 3–4, https://calhoun.nps.edu/bitstream/handle/10945/5123/10Sep_Callagy.pdf?sequence=1&isAllowed=y.

[41] Wexler, *New National Commitment Required*, 63.

[42] Rhodes et al., *Evaluation of the Multijurisdictional Task Forces*, 1.

[43] Eric S. Jefferis et al., "An Examination of the Productivity and Perceived Effectiveness of Drug Task Forces," *Police Quarterly* 1, no. 3 (September 1998): 86, https://doi.org/10.1177/109861119800100306; Reaves, *Local Police Departments, 2013*, 10.

the effectiveness of the conventional task forces model for combatting crimes.[44] A more recent study conducted in 2009 attempted to correlate the effectiveness of conventional crime task forces using data related to the number of cases investigated, arrests, and prosecutions; however, the researchers cautioned that "an unquantifiable amount of measurement error" was associated with the data collected.[45] Marcum et al. concluded that specialized child pornography cyber task forces (CTFs) were associated with an increased likelihood of detection resulting in more investigations and arrests.[46] Although the limited available literature related to the conventional task forces model provided some compelling arguments for them, it lacked empirical data and a comparative analysis to other available models or strategies to support the arguments.

3. Hybrid Task Forces Models

The available literature related to the hybrid task forces model, as defined in this study, was the most limited compared to the other two models. Most of the literature was on related topics as opposed to the specific subject matter. The United States Secret Service's Electronic Crimes Task Force (ECTF), one of the hybrid task forces models described in this study, joins multiple agencies from all levels of law enforcement together with private sector partners across the nation and internationally to share information and increase cybercrime investigative resources for the purpose of disrupting cybercriminals.[47] Bednar, Katos, and Hennell argue that the very nature of cybercrime investigations calls for multiagency collaboration to increase the investigative reach both across state lines and

---

[44] Jefferis et al., "An Examination of the Productivity and Perceived Effectiveness," 101; Brad W. Smith et al., "Multijurisdictional Drug Task Forces: An Analysis of Impacts," *Journal of Criminal Justice* 28, no. 6 (November 2000): 551, https://doi.org/10.1016/S0047-2352(00)00069-6.

[45] Rhodes et al., *Evaluation of the Multijurisdictional Task Forces*, 69.

[46] Catherine D. Marcum et al., "Policing Possession of Child Pornography Online: Investigating the Training and Resources Dedicated to the Investigation of Cyber Crime," *International Journal of Police Science & Management* 12, no. 4 (2010): 523, https://doi.org/10.1350%2Fijps.2010.12.4.201.

[47] United States Government Accountability Office, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO-07-705 (Washington, DC: United States, 2007), 27, https://www.gao.gov/new.items/d07705.pdf; Department of Homeland Security, *United State Secret Service Electronic Crimes Task Force* (Washington, DC: Department of Homeland Security, 2014), 2, https://www.dhs.gov/sites/default/files/publications/USSS_Electronic-Crimes-TaskForces.pdf.

internationally.[48] A 2017 BJA and PERF joint case study highlighted a unique cybercrime task forces model that fit the hybrid model as described in this study because of its decentralized characteristics and flexibility. The study examined a task forces model created by the Utah Department of Public Safety (UDPS) coined by PERF as the "Utah model."[49] The model was chosen for the case study because its holistic approach to cybercrime investigations that involved collaboration with private-sector, academia, and critical infrastructure.[50] Dolliver, Collins, and Sams conducted a 2017 study that consisted of a comparative analysis on eight "hybrid digital forensic task forces" throughout the United States that combined law enforcement agencies and academic institutions.[51] Although this study presented qualitative data highlighting the benefits of a collaborative hybrid cybercrime task forces model, it was a single narrowly study focused on hybrid models that had partnerships with academic institutions.[52] The currently available research regarding multijurisdictional collaborative policing efforts supports the concepts like the hybrid task forces model described in this study as a strategy for overcoming some of the complex challenges associated with cybercrime investigations.

Despite multiple scholarly documents validating collaborative efforts as effective strategies for addressing cybercrime investigations, research on the different types of collaborative efforts remains incomplete. Specifically, no known research is available into the benefits or drawbacks of the hybrid task forces model as defined for this study. The available body of related work in this area lacks comparisons between the different collaborative efforts or the use of internal resources. It also lacks comprehensive data or empirical evidence on the advantages and disadvantages of participation in these types of unique task forces models. Even though the report on the Utah model boasts the smart practices embedded in it, it lacks direct reference on how the model affects the cybercrime investigative capabilities or capacity for the participating agencies. Even though the focus

---

[48] Bednar, Katos, and Hennell, "The Complexity of Collaborative Cyber Crime Investigations," 217.

[49] Police Executive Research Forum, *The Utah Model*, 1–2.

[50] Bureau of Justice Assistance, *The Utah Model*, 5–9.

[51] Dolliver, Collins, and Sams, "Hybrid Approaches to Digital Forensic Investigations," 126–28.

[52] Dolliver, Collins, and Sams, 129.

on the Utah model provided compelling arguments for its effectiveness, it was a single case study and lacked comparative analysis to other existing strategies or models for addressing cybercrime investigative needs. The available research related to the hybrid models described in this study is underdeveloped.

4. LEMAS: Its Strengths and Drawbacks

Most statistical data used in this study came from the BJS LEMAS surveys that have considerable strengths and weaknesses. Due to relying on LEMAS statistics for the quantitative data in this study, it was included in the literature review. LEMAS provides robust data on local law enforcement agencies and have high response and survey completion rates.[53] LEMAS surveys have been conducted periodically since 1987 and represent data aggregated from over 3,000 local and state law enforcement agencies. The BJS requests data from all local law enforcement agencies with 100 or more officers and with a random sampling of smaller agencies.[54] The surveys categorize local law enforcement agencies by:

- agencies with 100 or more officers or those that serve populations of 100,000 or more
- agencies with 99 or fewer officers or those that serve populations of less than 100,000.[55]

The surveys used for this study represent data collected in 2013 and 2016. The 2013 survey had an 88 percent response rate, and the standard error percentages for the data used in this study were low, less than 1.5.[56] The 2016 survey had an 81.7 percent response rate, and

---

[53] Robert H. Langworthy, "Lemas: A Comparative Organizational Research Platform," *Justice Research and Policy* 4, no. 1–2 (December 1, 2002): 35–36, https://doi.org/10.3818/JRP.4.1.2002.21.

[54] "Law Enforcement Management and Administrative Statistics (LEMAS) Series," National Archive of Criminal Justice Data, accessed November 19, 2019, https://www.icpsr.umich.edu/icpsrweb/NACJD/series/92.

[55] Reaves, *Local Police Departments, 2013*, 9; Hyland and Davis, *Local Police Departments, 2016*, 10.

[56] Reaves, 11–21.

standard error percentages for the data used in this study were less than 2.30.[57] Due to issues related with the accuracy of respondent answers to the survey questions and some gaps in data collection, some of the reliability of LEMAS can be challenged.[58] Despite the questions regarding reliability, the LEMAS reports have been and continue to be trusted sources for law enforcement data.

D. RESEARCH DESIGN

The research for this study was used to examine three models being employed by local law enforcement agencies to address the need for cybercrime investigative capabilities and capacity: having internal resources, participation in conventional multijurisdictional task forces, and participation in hybrid multijurisdictional task forces. Most local law enforcement agencies that have cybercrime investigative capabilities and capacity employ one of or a combination of the models described in this study.

In addition to information obtained from the literature, a survey in the form of a questionnaire was sent to a sample of local law enforcement agencies and both conventional and hybrid cybercrime task forces was distributed to a small sample group. (see the Appendix for the questionnaires used in the survey.) Of the 32 questionnaires distributed, 14 of the surveyed agencies responded for a response rate of 43.7 percent.

Local law enforcement agencies and regional task forces from the State of California, which fit the conventional task forces model as defined for this study, made up most of the sample. This representation is significant to the study, as California accounts for the highest number of cybercrime victims in the nation.[59] Some of the agencies that responded requested that their agency not be named in this study. These agencies are referenced by size as described previously and general location or region. See Tables 1 and 2 for the agencies and task forces used in the survey. Although the response rate was too low to validate the sample, inconclusive, and not comprehensive enough, to determine a

[57] Hyland and Davis, *Local Police Departments, 2016*, 13–20.

[58] Langworthy, "Lemas," 36.

[59] Internet Crimes Complaint Center, *2018 Internet Crime Report*, 21.

common operating picture, the responses to the questionnaires were useful for shrinking gaps in the available open-source information.

For the purposes of this study, the term local law enforcement agency was used for police departments, sheriff's offices and departments, and investigative branches of district attorney's offices. Agencies with fewer than 60 officers or serving populations of fewer than 60,000 were referred to as "small," agencies with between 60 and 99 officers or serving populations between 60,000 and 99,000 were referred to as "midsize," and those agencies with more than 99 officers or serving populations of more than 99,000 were referred to as "large."

Table 1. Respondent Agencies of the Survey

AGENCY	SIZE
Belmont, CA. Police Department	Small
East Palo Alto, CA. Police Department	Small
Hillsborough, CA. Police Department	Small
Monterey County, CA. District Attorney's Office Investigations Bureau	Small
*Police Department in Southern California	Midsize
Mountain View, CA. Police Department	Midsize
*Police Department in Northern California	Midsize
Redwood City, CA. Police Department	Midsize
Indianapolis Metropolitan Police Department	Large
Police Department in Oklahoma	Large
Santa Clara County Sheriff's Office	Large

*Agencies requested they not be named in the study.

Table 2. Respondent Task Forces of the Survey

TASK FORCE	TYPE	LOCATION
Computer and Technology Crime High Tech Response Team (CATCH)	Conventional-Regional	Southern California
Electronic Crimes Task Force (ECTF)	Hybrid-Federal	San Francisco Field Office Area
Northern California Computer Crimes Task Force (NC3TF)	Conventional-Regional	Northern California

This study uses the SWOT analysis framework to examine three models for addressing cybercrime investigative capabilities and capacity described in this study. SWOT is an acronym for strengths, weaknesses, opportunities, and threats. It is applicable to this study because it provides a simple collection method that considers both internal and external factors that influence an organizational environment.[60] The SWOT analysis model has been in use for over 50 years.[61] SWOT provides a longstanding and recognized framework to extract comparative data about the three models for addressing cybercrime investigative capabilities and capacity described in this study.

The scope of this study focuses on three models used by local law enforcement agencies for increasing cybercrime investigative capabilities and capacity:

- internal resources
- conventional task forces
- hybrid task forces

[60] David W. Pickton and Sheila Wright, "What's SWOT in Strategic Analysis?," *Strategic Change* 7, no. 2 (1998): 102–3, https://doi.org/10.1002/(SICI)1099-1697(199803/04)7:2%3C101::AID-JSC332%3E3.0.CO;2-6.

[61] Marilyn M. Helms and Judy Nixon, "Exploring SWOT Analysis—Where Are We Now? A Review of Academic Research from the Last Decade," *Journal of Strategy and Management* 3, no. 3 (2010): 215–18, https://doi.org/10.1108/17554251011064837.

As used in this study, capabilities are the range of cybercrime investigative functions an agency can perform based on available resources, and capacity is the amount of available resources.[62] In the context of cybercrime investigative functions, resources include personnel with the necessary specialized training, specialized tools (equipment and software), and funding. The analysis focused on three key attributes of each of the three models that had the most significant influence over cybercrime investigative capabilities and capacity:

- level of cybercrime-investigative training and expertise development for personnel
- prioritization of cybercrime-related cases
- funding sources

The research for this study largely built on qualitative data from previous studies. Due to their nontraditional nature, traditional metrics for measuring the effectiveness of cybercrime investigative strategies are not always accurate and do not take into account variables unique to these complex investigative tasks.[63] Challenges with obtaining digital evidence and jurisdictional reach often equate to a disproportionate amount of criminal cases opened in relation to the amount case referrals.[64] Furthermore, statistics related to cybercrime arrests and case clearances are limited or not readily available via open-source documents and national crime reporting repositories, such as the FBI's Uniformed Crime Reporting (UCR) Program and the National Incident-Based Reporting System (NIBRS).[65] Traditional metrics are not an accurate way of gauging the effectiveness of cybercrime investigative efforts.

---

[62] Joseph W. Pfeifer and Ophelia Roman, "Tiered Response Pyramid: A System-Wide Approach to Build Response Capability and Surge Capacity," *Homeland Security Affairs* 12, art. 5 (December 2016): 4, https://www.hsaj.org/articles/13324.

[63] Police Executive Research Forum, *The Utah Model*, 34.

[64] Police Executive Research Forum, 34–35.

[65] Wexler, *New National Commitment Required*, 13.

The success of cybercrime investigative efforts requires the use of metrics not solely based on arrests and criminal prosecutions. Examples include the use of victim-centered metrics not based solely on arrests and prosecutions, such as the disruption of major criminal networks, loss recovery for victims, specialized training offered, and prevention of additional victimization as a result of cybercrime intelligence gathered and shared.[66] Australia's *National Plan to Combat Cybercrime* measures the capabilities and capacity of government agencies to address cybercrimes in terms of predicting, preventing, and disrupting them.[67] For these reasons, this study focused on the attributes of the three different models that correlated with their cybercrime investigative capabilities and capacity.

The results of the SWOT analysis were: (1) a qualitative assessment of the three different models described in the study, (2) recommendations for local law enforcement decision makers to consider when developing policies and protocols to address cybercrime investigative capabilities and capacity, and (3) recommendations for future research.

E. CHAPTER OVERVIEW

Chapter II provides a summary of the three models—internal resources, conventional task forces, and hybrid task forces—examined in this study. The different models are defined within the scope of the study and examples are provided for context. The chapter discusses how local law enforcement agencies employ the different models and provides some relevant data and background information.

Chapter III examines each of the models using the SWOT analysis framework to assess attributes related to cybercrime investigative capabilities and capacity. These attributes are the amount of training provided to assigned personnel that develops their technical expertise, how case referrals are prioritized, and funding sources. A combination of open-source information, the literature reviewed, and information obtained from the

---

[66] Police Executive Research Forum, *The Utah Model*, 34–35.

[67] Commonwealth of Australia, *National Plan to Combat Cybercrime* (ACT, Australia: Commonwealth of Australia, 2013), 17, https://sherloc.unodc.org/res/cld/lessons-learned/aus/national-plan-to-combat-cybercrime_html/National_Plan_to_Combat_Cybercrime.pdf.

questionnaires (listed in the Appendix of this study) provide context for significant strengths, weaknesses, opportunities, and threats associated with each of the models.

Chapter IV concludes the study by describing the main findings of the SWOT analysis of the three models and making recommendations for local law enforcement decision makers to consider when forming policies and protocols related to how their agencies will address the need cybercrime investigative capabilities and capacity. The chapter closes by answering the research question and making future research recommendations.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE DIFFERENT MODELS: INTERNAL RESOURCES, CONVENTIONAL TASK FORCES, AND HYBRID TASK FORCES

This chapter explains the three models—internal resources, conventional task forces, and hybrid task forces—as they have been defined and categorized for this study. In addition to providing background information about the models, the chapter concludes that these models or a combination thereof have been adopted by many local law enforcement agencies as a means of having cybercrime investigative capabilities and capacity.

A. INTERNAL RESOURCES

"Internal resources" as used in this study refers to local law enforcement agencies that have dedicated cybercrime units or other designated personnel who perform a range of cybercrime investigative functions ranging from digital forensics to cyber-related investigations. In this model, funding for specialized training and tools comes primarily from internal sources but can be supplemented by external sources, such as grants. The prioritization of cases is solely dictated by organizational or jurisdictional factors.

Dedicated cybercrime units have been adopted by multiple local law enforcement agencies as a strategy for internal cybercrime investigative capabilities and capacity. A 2016 study revealed that the formation or use of cybercrime units had tripled between 2000 and 2013.[68] Environmental factors (i.e., population served and regional orientation) and organizational factors (i.e., size and amount of specialization) influence whether a local law enforcement agency has a dedicated cybercrime unit.[69] For example, large departments are more likely to have dedicated cybercrime units than small ones.[70] The 2013 BJS LEMAS survey—that designated "small" agencies as those with 99 or fewer officers and "large" agencies as those with 100 or more officers—revealed that 39 percent

[68] Willits and Nowacki, "The Use of Specialized Cybercrime Policing Units," 23.

[69] Hamdi Yesilyurt, "The Response of American Police Agencies to Digital Evidence" (PhD diss., University of Central Florida, 2011), 157–58, https://stars.library.ucf.edu/etd/1732; Willits and Nowacki, "The Use of Specialized Cybercrime Policing Units," 24.

[70] Willits and Nowacki, 24.

of large local law enforcement agencies had personnel assigned to dedicated cybercrime units, which was a 20 percent increase from 2003. The same study also revealed only six percent of small to midsize agencies had personnel assigned to dedicated cybercrime units.[71] All three of the large agencies that responded to our survey had their own internal cybercrime investigative resources. Of all the factors, size has a direct correlation as to whether a local law enforcement agency will have a dedicated cybercrime unit.

The size and makeup of cybercrime units depend on organizational factors related to the local law enforcement agency. Some agencies have a single person assigned to their equivalent of a dedicated cybercrime "unit" while others have multiple people.[72] For example, the survey revealed that the Monterey County, California, District Attorney's Office Investigations Bureau (MCDABI), which has 32 employees, has one employee assigned to its digital forensic lab, supported by three sworn investigators who assist the lab in conjunction with regular investigative duties. The Montgomery County, Maryland, Police Department, which has approximately 1,900 employees, has five fulltime digital forensics examiners assigned to its dedicated Electronic Crimes Unit. Five detectives, who are assigned to different units throughout the department, serve as part-time digital forensics examiners and supplement fulltime examiners.[73] Some agencies use civilian staff with specialized computer skills to perform technical functions, such as digital forensics, in support of sworn investigators.[74] Local law enforcement agencies use a variety of staffing models in their cybercrime units.

Local law enforcement agencies without dedicated cybercrime units often have other personnel capable of performing cybercrime investigatory functions. The 2013 LEMAS survey revealed that 36 percent of large and 20 percent of small- to midsize- sized

---

71 Reaves, *Local Police Departments, 2013*, 9–10.

72 Stambaugh et al., *Electronic Needs Assessment*, 12.

73 Wexler, *New National Commitment Required*, 55; "Montgomery County Maryland Operating Budget: Police," Montgomery County Maryland Operating Budget, accessed September 30, 2019, https://apps.montgomerycountymd.gov/BASISOPERATING/Common/Department.aspx?ID=47D.

74 Teri A. Flory, "Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies" (master's thesis, Purdue University, 2015), 13, https://docs.lib.purdue.edu/open_access_theses/1220; Wexler, *The Role of Local Law Enforcement*, 27.

local law enforcement agencies, without dedicated cybercrime units, had other designated personnel to perform cybercrime investigatory functions.[75] In 2003, roughly 32 percent of large agencies had designated personnel for this function. The 2013 LEMAS findings also revealed that small to midsize agencies were more likely to have designated personnel for performing cybercrime investigative functions over a dedicated unit, whereas large agencies were more likely to have a dedicated cybercrime unit.[76] Even agencies without dedicated cybercrime units have taken steps to increase their cybercrime investigative capabilities and capacity.

Local law enforcement agencies deploy their cybercrime investigative resources in different ways depending on organizational needs. The Patterson Police Department, a large local police agency in New Jersey, uses a decentralized approach to cybercrime investigative capabilities and capacity by pairing tech-savvy detectives with more experienced detectives who have expertise in traditional investigations.[77] By the same token, from the survey, the Hillsborough Police Department, a small local police department in California, uses its general crimes detectives to perform cybercrime investigative functions. Other sworn specialists, who have extra training in digital forensics, augment the detectives and assist with more complex cyber investigations. The available research supports that having internal cybercrime resources has been an accepted practice by many small and midsize to large local law enforcement agencies for improving cybercrime investigative capabilities and capacity.

Whether they have dedicated units or other designated personnel, many local law enforcement agencies have accepted the need to have internal resources to address cybercrime investigative functions. A 2013 LEMAS report showed a 17 percent increase in the number of dedicated cybercrime units for large law enforcement agencies between 2003 and 2013, as shown in Figure 1.[78] Thus, in 2003, 59 percent, and in 2013, 76 percent

---

75 Reaves, *Local Police Departments, 2013*, 9–10.

76 Reaves, 9.

77 Wexler, *New National Commitment Required*, 55.

78 Reaves, *Local Police Departments, 2013*, 10.

of large agencies, had either dedicated units or other designated personnel for cybercrime investigative duties.[79] Enough local law enforcement agencies have adopted internal cybercrime investigative resources to legitimize the practice among the local law enforcement community.

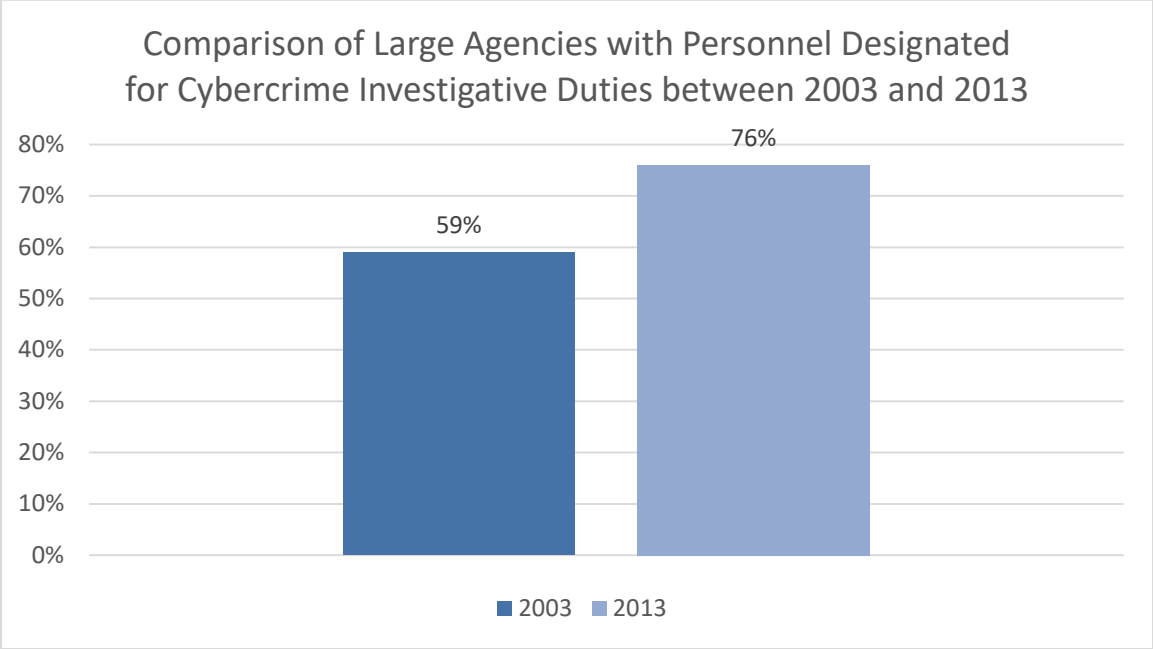


Figure 1. Comparison of Large Agencies between 2003 and 2013 with Personnel Designated for Cybercrime Investigative Duties.

B. CONVENTIONAL TASK FORCES

The conventional task forces model as used in this study refers to formal collaborative arrangements or agreements between two or more participating agencies for performing a range of cybercrime investigative functions ranging from digital forensics to cyber-related investigations. In this model, assigned personnel from different agencies are combined as one entity under the task forces and the majority of them work together from a centralized location. The home agency relinquishes the day-to-day control over their

[79] Reaves, 9–10.

assigned personnel to the task forces chain of command. Participating agencies receive full or partial salary reimbursement for personnel assigned to the task forces.

Local law enforcement agencies commonly use participation in conventional task forces as means to addressing complex crimes. This model has become increasing more popular over the years as a strategy for combatting a variety of crimes.[80] Tens of thousands of police officers from local law enforcement agencies around the nation participate in this type of task forces model.[81] Conventional task forces involve formal operational partnerships between multiple local, state, and federal law enforcement agencies for increased jurisdictional reach.[82] Participating agencies consolidate their resources in the task forces to perform regional cybercrime investigative functions.[83] Combining resources helps agencies increase their cybercrime investigative capabilities and capacity while minimizing the drain on any one agency's resources.

Narcotics task forces have been in existence for many years and law enforcement agencies of all sizes continue to participate in them. The formation of narcotics task forces became popular in the 1980s as an enforcement strategy to deal with the cross-jurisdictional and complex nature of narcotics trafficking crimes, which required coordination and collaboration between multiple law enforcement agencies from all levels.[84] Narcotics task forces have continued to grow in popularity since their inception.[85] The 2013 LEMAS data revealed that 49 percent of all agencies surveyed participated in narcotics task forces. Moreover, 100 percent of agencies serving populations of 1,000,000 or more participated in them, and 31 percent of agencies serving populations of 2,499 or fewer participated. This survey also revealed that 13 percent of local law enforcement agencies participated in gang task forces and four percent in human trafficking task forces, with large agencies

---

80 Rachel A. Harmon, "Federal Programs and the Real Costs of Policing," *New York University Law Review* 90, no. 3 (June 2015): 944.

81 Harmon, 944; Reaves, *Local Police Departments, 2013*, 10.

82 Stambaugh et al., Electronic Needs Assessment, 12.

83 Wexler, *New National Commitment Required*, 63.

84 Jefferis et al., "An Examination of the Productivity and Perceived Effectiveness," 86.

85 Smith et al., "Multijurisdictional Drug Task Forces," 551–53.

having higher percentages of participation in all.[86] The available research validated participation in conventional task forces as a widely used strategy by local law enforcement agencies for dealing with the challenges associated with complex crimes that span across jurisdictions.

Following the popularity of other task forces, conventional task forces for addressing cybercrime have become more popular over the years. With five regional cybercrime task forces located throughout the state, California cybercrime task forces provided a significant amount of data for this study.[87] All the regional cybercrime task forces in California have a designated lead agency that manages the administration of the task forces and has fiduciary responsibility.[88] The five regional cybercrime task forces are NC3TF, the Sacramento Valley Hi-Tech Crimes Task Force (SVHTCTF), the Rapid Enforcement Allied Computer Team (REACT), the Southern California High Tech Task Force (SCHTTF), and the Computer and CATCH.[89] Survey respondents from NC3TF and CATCH who shared that staffing for the task forces is comprised from agencies in the region. The size of the task forces and number of affiliate agencies depends on the region and the task forces composition includes local, state, and federal law enforcement officers.[90] Most cybercrime task forces fit into the conventional model described in this section.

---

86 Reaves, *Local Police Departments, 2013*, 10.

87 Xavier Becerra, "High Technology Theft Apprehension and Prosecution (HTTAP) Program," State of California Department of Justice, Office of the Attorney General, December 13, 2011, https://oag.ca.gov/ecrime/httap.

88 "About NC3TF," Northern California Computer Crimes Task Force, accessed May 18, 2019, https://www.nc3tf.org/about.

89 High Technology Crime Advisory Committee, *High Technology Crime in California—FY09/10* (Mather, CA: California Emergency Management Agency, 2010), 5, https://oag.ca.gov/sites/all/files/agweb/pdfs/ecrime/2010_httap_report.pdf.

90 "About Us," REACT—Regional Enforcement Allied Computer Team, accessed February 25, 2019, http://www.reacttf.org/reacttf/d/index.html?#/page/about; Northern California Computer Crimes Task Force, "About NC3TF"; "CATCH: Computer and Technology Crimes High Tech Task Force," CATCH, accessed May 18, 2019, https://catchteam.org/.

C. HYBRID TASK FORCES

Hybrid task forces as used in this study refer to formal collaborative arrangements or agreements between more than one participating agency that perform a range of cybercrime investigative functions from digital forensics to cyber-related investigations. This model mostly decentralized in makeup as assigned personnel have the flexibility to work from their home agencies or separate locations. Participation in this task forces model has benefits related to specialized training and equipment and may include limited funding assistance in the form of asset forfeiture sharing and reimbursement of some personnel costs. The home agency maintains the majority of day-to-day control over its personnel assigned to the task forces.

The United States Secret Service's ECTF fits the description of hybrid task forces as used in this study. The ECTF is a network of more than 2,500 investigators from international, federal, state, and local law enforcement agencies connected to each other through this hybrid task force model, as well as to academic and private-sector partners.[91] ECTFs number 39 throughout the United States, as well as one in London, and one in Rome that allow them to focus on regional issues.[92] Per our survey's responses, the ECTF allows participating agencies to choose who is assigned to the task force while they work from their home agencies in either a full- or part-time capacity. The decentralized makeup of the ECTFs allows for a large network of member agencies that collectively support one another with cybercrime investigative tasks on an ad hoc basis.[93] Our survey responses confirmed that small, midsize, and large agencies participate in the ECTF. The ECTF provides agencies with a way to supplement their internal resources, as well as an alternative to participation in a conventional task forces model.

---

[91] Michael Breslin, "The U.S. Secret Service Electronic Crimes Task Forces: Employing Public-Private Sector Partnerships to Combat Cybercrime," *Police Chief*, 52–54, July 2017, https://www.policechiefmagazine.org/wp-content/uploads/PoliceChief_July2017_F-web.pdf.

[92] Breslin, 53; Department of Homeland Security, *United States Secret Service Electronic Crimes Task Force*, 1–2.

[93] Department of Homeland Security, 1–2.

For this study, UDPS's Utah Cyber Crimes Task Force (UCCTF) fits the hybrid task forces model because of its nontraditional and mostly decentralized makeup. The UCCTF combines a cybercrimes unit from UDPS with resources from federal law enforcement and other government agencies that work together from separate locations.[94] The UCCTF, also referred to as the "Utah model," benefits from robust partnerships that improve the capabilities and capacity of the model.[95] The Utah model is a partnership between the Cyber Crime Unit of the UDPS' State Bureau of Investigation (SBI), the Utah Statewide Information and Analysis Center (SIAC), the Utah State Department of Technology Services (DTS), the Department of Homeland Security (DHS), and the FBI. The UCCTF has two civilian employees, a cyber intelligence analyst, who is located at the SIAC, and a digital forensics analyst, who is located in the region's Regional Computer Forensics Laboratories (RCFL). Civilian private-sector partners serve as subject matter experts for relevant information sharing, and for threat advisories (See Table 1).[96] As well as combining centralized and decentralized aspects of a collaborative effort, the UCCTF is both multidisciplinary and multijurisdictional.

Operations Wellspring (OWS) is a unique component of the Utah model that integrates SBI with the FBI. Through OWS, the SBI Cyber Crimes Unit, which consists of one full-time sergeant and two full-time detectives, partners with the FBI and is physically located in the FBI's Salt Lake City field office. OWS, which was piloted in Utah, has expanded to other states and is open to both state and local agencies.[97] The OWS partnership differs from traditional federal collaborative efforts, as no federal funding is associated with it.[98] SBI Cyber Crimes Unit's participation in OWS was another nontraditional aspect of the UCCTF hybrid model. See Figure 2.

---

[94] Police Executive Research Forum, *The Utah Model*, 5–6.

[95] Police Executive Research Forum, 2–6.

[96] Police Executive Research Forum, 5–6.

[97] Police Executive Research Forum, 38.

[98] Police Executive Research Forum, 64.

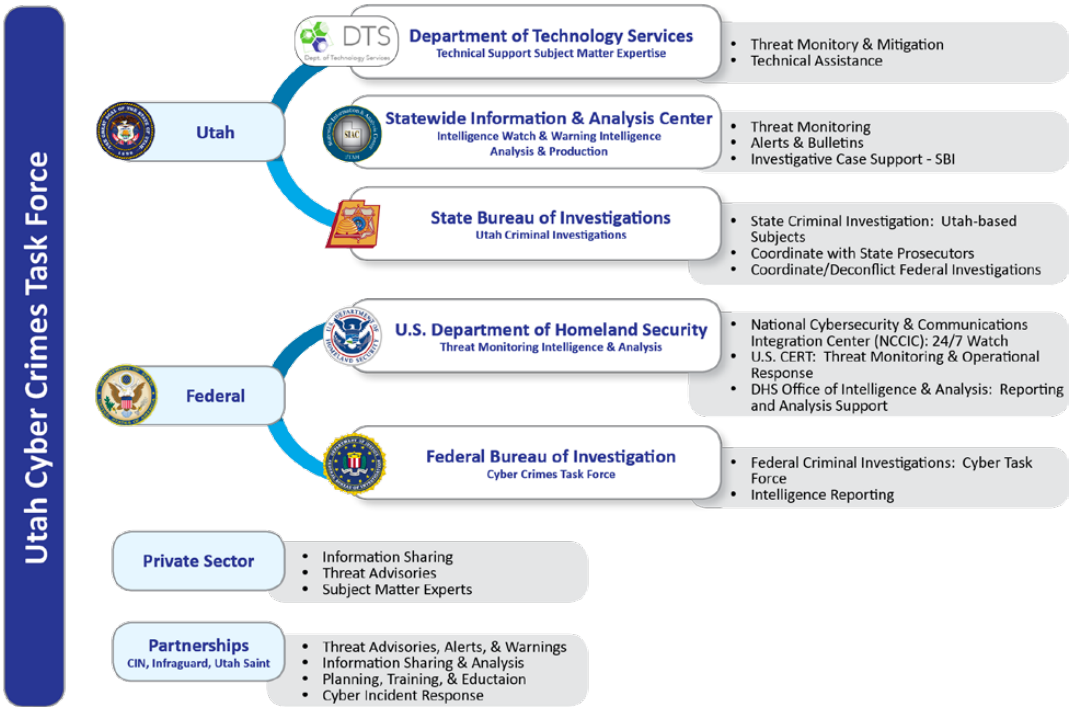


Figure 2. Agency Involvement in the Utah Cyber Crimes Task Force.[99]

The UCCTF is the only task force in this study that has staff assigned to a regional fusion center. Many of the nation's fusion centers have cyber-focused analysts and other staff who provide information on cybercrime and cybersecurity trends to law enforcement agencies and other fusion center partners.[100] The integration of multiple levels of law enforcement and private sector partners makes fusion centers ideal for the sharing of important cybercrime and cybersecurity related information.[101] The UCCTF's cyber analyst assists investigators by sharing cyber-related criminal intelligence and vetting incoming cases to determine the criminal nexus and if enough evidence is available to open

---

[99] Source: Police Executive Research Forum, *The Utah Model*, 1–2.

[100] Department of Homeland Security, *2017 National Network of Fusion Centers Final Report* (Washington, DC: Department of Homeland Security, 2017), 4, https://www.dhs.gov/sites/default/files/publications/2017_National_Network_of_Fusion_Centers_Final%20Report.pdf.

[101] Global Advisory Committee, *Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers* (Washington, DC: Global Advisory Committee, 2015), 5, https://it.ojp.gov/GIST/178/File/Cyber%20Integration%20for%20Fusion%20Centers.pdf/.

an investigation.[102] Having a task forces member assigned to the SAIC makes sense for both cyber threat and criminal intelligence sharing.

D. CONCLUSION

Internal resources, conventional task forces, and hybrid task forces as described in this chapter are all accepted models for addressing the challenges related to cybercrime investigative functions. Multiple local law enforcement agencies have adopted one or a combination of the three different models describe in this study for addressing cybercrime investigative capabilities and capacity. In Chapter III, the three different models are examined in terms of investigative capabilities and capacity using the SWOT analysis framework.

[102] Police Executive Research Forum, *The Utah Model*, 31.

III. ANALYSIS OF THE THREE MODELS: INTERNAL RESOURCES, CONVENTIONAL TASK FORCES, AND HYBRID TASK FORCES

In this study, SWOT analysis was used to make general comparisons between the three models to derive conclusions about how they impact the cybercrime investigative capabilities and capacity of local law enforcement agencies. The level of cybercrime training and expertise development for assigned personnel, prioritization of cybercrime investigations, and funding sources are compared relative to each model based solely on the findings from the research conducted for this study. The analysis was based only on the open-source information obtained during the research for this study and was not intended to be an exhaustive all-inclusive list of the strengths, weaknesses, opportunities, and threats associated with each model. Only significant characteristics for each category in the framework are described. The analysis is intended to add to the limited body of research in this space.

A. INTERNAL RESOURCES

This section uses open-source information from the literature reviewed, government documents, and responses from the questionnaires in Section D of Chapter I to analyze how the internal resources model impacts cybercrime investigative capabilities and capacity using the SWOT framework.

1. Strengths

When compared to the task forces models in this study, a strength of the internal resources model is an agency having full autonomy to prioritize cases. Agencies have the ability prioritize cybercrime investigative efforts based on specific jurisdictional needs related to community impact and workload capacity.[103] Agencies with their own internal cybercrime resources have more flexibility with how they prioritize cases and are not otherwise tethered to multijurisdictional task forces protocols for or outside agency influence over case

[103] Stambaugh et al., *Electronic Needs Assessment*, 12; Willits and Nowacki, "The Use of Specialized Cybercrime Policing Units," 6–8.

prioritization.[104] The flexibility to prioritize cybercrime investigations specific to departmental needs ensure local law enforcement agencies are accountable to the communities they serve.[105] As revealed in our survey responses, agencies with their own internal cybercrime investigative resources are able to prioritize cases based on the specific type and jurisdictional needs at the time.

A successful investigation involving the Metropolitan Nashville, TN Police Department (MNPD) provides an example of how the ability to prioritize investigations based on jurisdictional needs leads to successful and timely cyber-related investigative actions. In 2013, the MNPD investigated a high-profile sexual assault investigation involving a 21-year-old female student from Vanderbilt University, who was drugged and raped by four members of the football team. The success of the investigation hinged on the timely collection and analysis of digital evidence consisting of videos and photos taken during the sexual assault that were shared via text messages between one of the suspects and an individual in Riverside, California. Since the MNPD had internal cybercrime resources, the necessary investigative steps were prioritized that allowed critical digital evidence to be collected and analyzed in a timely manner. This evidence, ultimately, led to the identification of multiple suspects, their arrests, and subsequent criminal prosecution.[106] This case was successful because of the MNPD's ability to prioritize the necessary cybercrime investigative task forces in a manner that met their needs.

2. Weaknesses

As compared to the task forces models, internal cybercrime investigative resources often have capacity challenges in keeping up with the workload. Many local law enforcement agencies are faced with significant capacity challenges associated with a shortage of personnel and technical tools to meet the demand for cybercrime-related investigative support and turn

[104] Police Executive Research Forum, *The Utah Model*, 18.

[105] Harmon, "Federal Programs and Real Costs," 945.

[106] Wexler, *New National Commitment Required*, 35–36.

to task forces models to help overcome the challenges.[107] Limited cybercrime investigative expertise in most local law enforcement agencies, coupled with the cyber-elements that are part of almost every traditional crime investigation today, has caused a significant increase in the workload of cybercrime investigative specialists.[108] Due to a lack of understanding regarding workload and capacity challenges associated with cybercrime investigative functions, executive leadership in many departments have failed to make having such capabilities a priority.[109] Unlike multijurisdictional models that control workload based on case prioritization protocols to prevent wasting time-consuming investigative efforts, agencies with internal resources are more beholden to jurisdictional-specific expectations for and political influence over which cases to investigate or prioritize.[110] Agencies with internal cybercrime investigative resources face similar challenges related to the workload capacity of their available resources.

Evidence of workload capacity challenges associated with the internal resources model can be found in data from scholarly studies and agency-specific reports. In a 2018 study involving two large Australian police agencies, personnel serving in cybercrime investigative roles reported an annual increase from 3,500 to 4,000 in cases referred and noted how the cases were more complex, which thus increased the amount of time needed to process them.[111] Between 2017 and 2019, the Computer and Digital Forensic Unit (CDFU) of the Indianapolis Metropolitan Police Department (IMPD) experienced a 42.8 percent increase in

---

[107] Goodison, Davis, and Jackson, *Digital Evidence and the U.S. Criminal Justice System*, 23; Wexler, *New National Commitment Required*, 62–64.

[108] Harkin, Whelan, and Chang, "The Challenges Facing Specialist Police Cyber-Crime Units," 523–24.

[109] Harkin, Whelan, and Chang, 525.

[110] Harmon, "Federal Programs and Real Costs," 944–45; Police Executive Research Forum, *The Utah Model*, 18.

[111] Harkin, Whelan, and Chang, "The Challenges Facing Specialist Police Cyber-Crime Units," 524.

forensic examinations.[112] The data illustrates the rising workload capacity challenges faced by agencies with internal cybercrime investigative resources.

3. Opportunities

Opportunities exist to improve the capabilities and capacity of the internal resources model by increasing basic cybercrime investigative knowledge throughout the agency. Cybercrime specialists can avoid hours of wasted time triaging digital devices and attempting to recover evidence when first responders and detectives, who are trained in basic cybercrime investigative techniques, assess and preserve digital devices with evidentiary value.[113] Considering most cyber-related investigations begin with patrol officers, their ability to conduct preliminary investigative steps is critical to the success of any further investigative actions by specialists.[114] Training patrol officers in basic cybercrime investigative functions represents a significant opportunity to enhance an agency's cybercrime investigative capabilities and capacity as patrol functions represent about 70 percent of operations for most local law enforcement agencies.[115] Despite the data, a 2013 BJS study of 664 state and local law enforcement agencies revealed that trainees were only receiving three hours of cybercrime-related training in the basic academy.[116] The research supports arguments for agencies with internal resources to provide more cybercrime investigative training and expertise development opportunities for first responders and other personnel who do not serve in cybercrime investigative roles.

---

[112] Indianapolis Metropolitan Police Department, *IDMP Quarterly Report:First Quarter 2019* (Indianapolis, ID: Indianapolis Metropolitan Police Department, 2019), 11; Indianapolis Metropolitan Police Department, *IDMP Quarterly Report: Second Quarter 2019* (Indianapolis, ID: Indianapolis Metropolitan Police Department, 2019), 12; Indianapolis Metropolitan Police Department, *IDMP Quarterly Report: Third Quarter 2019* (Indianapolis, ID: Indianapolis Metropolitan Police Department, 2019), 12; Indianapolis Metropolitan Police Department, *IDMP Quarterly Report: Fourth Quarter 2019* (Indianapolis, ID: Indianapolis Metropolitan Police Department, 2019), 12; Indianapolis Metropolitan Police Department, *IDMP 2017 Annual Report* (Indianapolis, ID: Indianapolis Metropolitan Police Department, 2017), 66.

[113] Police Executive Research Forum, *The Utah Model*, 27.

[114] Sameer Hinduja, "Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future," *International Journal of Cyber Criminology* 1, no. 1 (2007): 7, https://doi.org/10.5281/zenodo.18275; Wexler, *New National Commitment Required*, 59.

[115] Bandl, "The Characteristics and Structure of Police," 52.

[116] Reaves, *State and Local Law Enforcement Training Academies, 2013*, 7.

Some agencies have already prioritized the need to spread cybercrime investigative expertise throughout their organizations by providing cyber-related training to staff who do not serve in specialized cybercrime investigative roles. The Patterson, NJ Police Department has personnel with cybercrime investigative capabilities and capacity in all of its detective units to ensure these resources are more readily available.[117] Per our survey, the Santa Clara County, CA Sheriff's Office (SCCSO) reports having more personnel available to assist their cybercrime specialists by providing their patrol deputies with 40 hours and detectives with up to 100 hours of both formal and informal training in cybercrime investigative techniques. Montgomery County, MD Police Department trains officers in the academy how to identify and triage devices that may have digital evidentiary value, which has resulted in the weeding out of digital devices that do not require analysis by specialists.[118] First responders and detectives with cybercrime investigative skills increase the internal cybercrime investigative capabilities and capacity of an agency.

4. Threats

Agency and other funding necessary for cybercrime investigative resources is an ongoing threat to the internal resource model. An agency's commitment to maintaining in-house cybercrime investigative capabilities and capacity is determined by the amount of funding set aside for essential ongoing expenses.[119] Ongoing funding challenges have been a significant argument for individual local law enforcement agencies to consolidate and unify efforts.[120] In a 2014 PERF report, 31 percent of agencies surveyed cited a lack of funding for internal cybercrime investigative resources.[121] The findings of the PERF study were supported by another 2014 study that revealed how local law enforcement agencies faced funding challenges that compromised their ability to maintain essential digital evidence tools

---

117 Wexler, *New National Commitment Required*, 55.

118 Wexler, 60–61.

119 Greg Gogolin and James Jones, "Law Enforcement's Ability to Deal with Digital Crime and the Implications for Business," *Information Security Journal: A Global Perspective* 19, no. 3 (2010): 110, https://doi.org/10.1080/19393555.2010.483931.

120 Callagy, "Can Local Police and Sheriff's Departments Provide a Higher Degree of Homeland Security Coordination and Collaboration Through Consolidation of Police Services?," 3–4.

121 Wexler, *The Role of Local Law Enforcement*, 7.

and software packages for performing cybercrime investigative functions.[122] As revealed from responses to our survey from the MCDABI, even agencies that have their own internal resources rely on outside funding to offset the cost of equipment. Agencies that rely on internal resources continue to be susceptible to budgetary challenges that impact their cybercrime investigative capability and capacity.

B. CONVENTIONAL TASK FORCES

This section uses open-source information from the literature reviewed, government documents, and responses from the questionnaires in Section D of Chapter I to analyze how the conventional task forces model impacts cybercrime investigative capabilities and capacity of participating agencies using the SWOT framework.

1. Strengths

When compared to the internal resources model and hybrid task forces model, a strength of participation in conventional cybercrime task forces is the amount of ongoing specialized training for assigned personnel. Research has identified a correlation between increased investigative productivity and the amount of training provided to task forces members.[123] Consolidation of resources has been credited with better and more uniformed training in addition to more exposure to a variety of different investigations.[124] Moreover, the centralized makeup of the conventional model increases opportunities for hands-on training between collocated personnel with differing levels of expertise.[125] Responses to our survey revealed that members of CATCH and NC3TF receive years of specialized training to qualify them in various cybercrime investigative disciplines and from their exposure to develop a high degree of specialized investigative expertise. Responses to the survey by NC3TF revealed that the task forces budgets approximately $62,000.00 annually for ongoing specialized training

---

[122] Goodison, Davis, and Jackson, *Digital Evidence and the U.S. Criminal Justice System*, 24.

[123] Catherine D. Marcum and George E. Higgins, "Combating Child Exploitation Online: Predictors of Successful ICAC Task Forces," *Policing: A Journal of Policy and Practice* 5, no. 4 (2011): 314, https://doi.org/10.1093/police/par044.

[124] Callagy, "Can Local Police and Sheriff's Departments Provide a Higher Degree of Homeland Security Coordination and Collaboration Through Consolidation of Police Services?," 45.

[125] Police Executive Research Forum, *The Utah Model*, 37.

to ensure members are highly skilled. An advantage of participating in a conventional task force is the amount of ongoing specialized training this task force provides.

Successful investigations involving complex cyber-related crimes illustrate the high level of training received and expertise developed by investigators assigned to conventional task forces. A 2019 investigation into a multijurisdictional crime ring involving the theft of data from smartphones by an elaborate SIM (subscriber identity module) card swapping scheme, highlights the level of training received by task forces investigators from REACT, a northern California task force.[126] The investigation led to the identification of multiple victims across the nation representing millions of dollars in loss and to the successful prosecution of the main suspect.[127] In 2010, highly skilled investigators from the SCHTTF conducted an identity theft investigation that led to the arrest of a suspect who was part of a West African criminal organization involved in a sophisticated data intrusion crime scheme.[128] These case examples showcase the cybercrime investigative capabilities of well-trained conventional task forces investigators.

2. Weaknesses

When compared to internal resources and hybrid task forces models, a weakness of the conventional task forces model is the case prioritization for participating agencies. Conventional task forces combine personnel from multiple agencies into an independent entity not controlled or governed by the individual jurisdictional and investigative needs of the participating agencies.[129] Most conventional task forces are accountable to grant funding performance data requirements that influence their investigative priorities.[130] Although the two conventional task forces that responded to our survey prioritize cases originating from the

---

[126] Stephen Stock et al., "Hackers Steal Millions from Bay Area Residents by Targeting Cellphones in 'SIM Swap' Scams," NBC Bay Area, May 23, 2019, https://www.nbcbayarea.com/news/local/hackers-steal-millions-from-bay-area-residents-by-targeting-cell-phones-in-sim-swap-scams/189712/; Brady Gavin, "What Is A SIM Card (And What Comes Next)?," *How-to Geek*, accessed July 22, 2020, https://www.howtogeek.com/353634/what-is-a-sim-card/.

[127] Stock et al., "Hackers Steal Millions."

[128] High Technology Crime Advisory Committee, *High Technology Crime in California*, 30.

[129] Harmon, "Federal Programs and Real Costs," 944–45.

[130] Rhodes et al., *Evaluation of the Multijurisdictional Task Forces*, 70.

home agencies of their assigned personnel, previous research contends that response delays for investigative requests from agencies with personnel assigned to task forces are still a factor.[131] Per SCCSO's responses to our survey, investigators assigned to the REACT Task Force may not always be able to prioritize cases referred by their home agencies based on their responsibility to investigate cases from other jurisdictions. Data from the High Technology Theft Apprehension and Prosecution (HTTAP) Program revealed that all five regional task forces in California investigated a combined total of 1,312 cyber-related cases and conducted a combined total of 1,244 forensic examinations in the 2009–2010 fiscal year.[132] When considering these five conventional task forces service jurisdictions spanning across 29 counties with a combined population of over 31 million and the 34,606 cybercrime complaints IC3 recorded for California in 2010, these numbers suggest that only a fraction of the cases from the multiple jurisdictions in their regions are being prioritized by the task forces.[133] A factor to consider when agencies are considering whether to participate in a conventional task force is the potential lack of control in how cases from their jurisdiction will be prioritized within said task force.

3. Opportunities

Opportunities exist to increase the investigative capabilities and capacity of the conventional task forces model by providing more cybercrime investigative-related training to the local law enforcement agencies within the task forces' regions of responsibility. Many of the cases adding to the workload of regional cybercrime task forces are referred by local law enforcement agencies within their region that lack the capabilities or capacity to perform any level of cybercrime investigative steps. This scarcity underscores the need for personnel from local law enforcement agencies to have the ability to recognize cases that should be referred to the task forces for further investigative work but also provide assistance with some

---

131 Wexler, *The Role of Local Law Enforcement*, 19–23; Police Executive Research Forum, *The Utah Model*, 18.

132 High Technology Crime Advisory Committee, *High Technology Crime in California*, 6.

133 High Technology Crime Advisory Committee, 5; National White Collar Crime Center, *California IC3 2010 Internet Crime Report* (Glen Allen, VA: National White Collar Crime Center, 2011), 1, https://www.ic3.gov/media/annualreport/2010/California%202010%20Report.pdf.

of the cybercrime investigative actions.[134] Training patrol officers and detectives from local law enforcement agencies in how to recognize devices that have digital evidentiary value and those that do not helps to reduce the backlog of digital evidence that impacts specialists assigned to task forces.[135] In 2009, an officer from San Jose Police Department correctly identified and seized card skimmers, digital devices used for unlawfully accessing credit card numbers, during a traffic stop. The officer's basic knowledge of digital devices with evidentiary value coupled with the simple initial investigative steps conducted led to an ongoing investigation by specialists from the REACT Task Force.[136] Training first responders and investigators from local law enforcement agencies in a conventional task force's region of responsibility serves as a force multiplier for the task forces specialists.

Providing cybercrime investigative training to personnel from agencies within their region should be a goal for every conventional task force. Previous studies involving local law enforcement agencies have reiterated the importance of regional cybercrime task forces providing more basic cyber-investigative training to local law enforcement agencies.[137] Training other law enforcement agencies in the identification and handling of suspected cybercrimes was a key objective for the REACT Task Force, as indicated in a 2009 HTTAP Progress Report.[138] The continued proliferation of cybercrimes that corresponds with technology advances and increased internet connectivity highlight the continued need for task forces to prioritize cybercrime training for members of local law enforcement agencies.[139] The research for this study validated the opportunities that exist for the conventional task forces model by providing training to personnel from the local law enforcement agencies.

---

134 Wexler, *New National Commitment Required*, 63–64.

135 Wexler, 59–61.

136 David Hendrickson, *High Technology Theft Apprehension & Prosecution Program Progress Report* (San Jose, CA: Santa Clara County District Attorney's Office, 2010), 7, https://info.publicintelligence.net/REACTOct-Dec09.pdf.

137 Sameer Hinduja, "Perceptions of Local and State Law Enforcement Concerning the Role of Computer Crime Investigative Teams," *Policing: An International Journal* 27, no. 3 (September 2004): 352, https://doi.org/10.1108/13639510410553103.

138 Hendrickson, "High Technology Theft Apprehension," 8.

139 Wexler, *New National Commitment Required*, 16.

4. Threats

Unlike the internal resources and hybrid task forces models, the conventional task forces model is dependent on external funding sources to operate. Conventional task forces need steady funding sources to keep up with training needs and for the cost of expensive cybercrime investigative software licenses and specialized technology.[140] As derived from the answers to our survey provided by NC3TF and CATCH, local law enforcement agencies that supply these task forces with personnel rely on funding from the task forces in return. A 2009–2010 HTTAP fiscal year report cited inadequate and decreased state funding for the five regional task forces in California as threatening their ability to maintain the cybercrime investigative capabilities and capacity necessary to keep up with the ever-evolving demands.[141] Any decreased funding to the task forces impacts the ability of the task forces to provide funding in return to participating agencies. Funding for the costly nature of maintaining the necessary resources conventional task forces need for keeping pace with cybercrime investigative demands remains an ongoing threat.

C. HYBRID TASK FORCES

This section uses open-source information from the literature reviewed, government documents, and responses from the questionnaires in Section D of Chapter I to analyze how the hybrid task forces model impacts cybercrime investigative capabilities and capacity of participating agencies using the SWOT framework.

1. Strengths

As compared to internal resources and conventional task forces models, a significant strength of participation in the hybrid task forces model is the ability for the agency to maintain a high degree of control over case prioritization while also receiving the benefits offered by the task forces model. Participating agencies receive some of the same resource and training benefits as participating agencies in conventional task forces without

---

[140] Marcum and Higgins, "Combating Child Exploitation Online," 315; Wexler, *New National Commitment Required*, 63.

[141] High Technology Crime Advisory Committee, *High Technology Crime in California*, 7.

compromising accountability to agency-specific hierarchy or the ability to investigative cases related to jurisdictional needs.[142] The hybrid task forces model provides a force multiplier by connecting specialized personnel from different agencies under a common umbrella while accounting for the specific jurisdictional investigative needs of participating agencies of varying sizes.[143] ECTF responses to our survey revealed how participating agencies dictate whether their assigned personnel serve the task forces on full-time or part-time basis. Moreover, the survey responses highlight how the ECTF provides participating agencies with free specialized equipment and training, as well as access to a national network of cybercrime experts to help them investigate their own cases. Through our survey, ECTF related how the task force has basic expectations on case prioritization based on threat and danger type, amount of loss, and significance of community impact.

UCCTF's association with OWS provides the SBI Cyber Crimes Unit with similar benefits related to training and control over case prioritization as the ECTF hybrid model. In addition to free cybercrime training courses, OWS provides UCCTF members hands-on training from FBI cybercrime experts with whom they work alongside while investigating jurisdictional-specific cases that would not otherwise meet the FBI's threshold for investigation.[144] The federal government-sponsored training for members of these hybrid task forces relieves the individual agencies of the financial burden associated with sending their personnel to the specialized training necessary to be effective in their roles.[145] The hybrid task forces model provides agencies that would benefit from participating in collaborative multijurisdictional efforts an alternative to the conventional task forces model.

2. Weaknesses

When compared to the conventional task forces model, the decentralized aspects of hybrid task forces are a weakness of the model. The collocation of specialized personnel from

---

[142] Harmon, "Federal Programs and Real Costs," 945.

[143] Callagy, "Can Local Police and Sheriff's Departments Provide a Higher Degree of Homeland Security Coordination and Collaboration through Consolidation of Police Services?," 25.

[144] Police Executive Research Forum, *The Utah Model*, 37–38.

[145] Goodison, Davis, and Jackson, *Digital Evidence and the U.S. Criminal Justice System*, 16.

multiple law enforcement agencies leads to more interagency cooperation and increased learning opportunities.[146] Personnel of the hybrid task forces model often work from different locations, which is not conducive to the type of hands-on training and mentorship common when mixing personnel of varying specialized skill levels into the same workspace.[147] The decentralized aspects of this model result in a lack of uniformity and less investigative coordination.[148] The lack of coordination that comes with participating agencies not being consolidated as with the conventional task forces model often leads to a duplication of effort.[149] As indicated in our survey responses from NC3TF and CATCH, uniformed training and increased investigative coordination between agencies are two of the perceived benefits of the conventional task forces model.

3. Opportunities

Opportunities exist for agencies that participate in hybrid task forces to maximize the benefits to the agency by spreading some cybercrime investigative responsibilities to personnel not assigned to the task forces. Like the conventional task forces model, personnel assigned to hybrid task forces face similar workload capacity challenges.[150] Allowing hybrid task forces members to focus on more complex investigative functions by offsetting less complex cyber-related tasks on patrol officers, traditional crimes detectives, and other personnel will help in increasing the capacity of task forces personnel and that of their respective agencies.[151] This capacity can be achieved through ensuring first responders and others not assigned to the task forces receive basic levels of cybercrime investigative training. As indicated by the responses to our survey, affiliation with ECTF provides participating agencies with the opportunity to send personnel to free training provided by the National

---

[146] Wexler, *New National Commitment Required*, 63; Police Executive Research Forum, *The Utah Model*, 63–64.

[147] Police Executive Research Forum, *The Utah Model*, 37.

[148] Callagy, "Can Local Police and Sheriff's Departments Provide a Higher Degree of Homeland Security Coordination and Collaboration Through Consolidation of Police Services?," 3–4.

[149] Callagy, 27.

[150] Goodison, Davis, and Jackson, *Digital Evidence and the U.S. Criminal Justice System*, 23.

[151] Hinduja, "Computer Crime Investigations in the United States," 7; Goodison, Davis, and Jackson, *Digital Evidence and the U.S. Criminal Justice System*, 17.

Computer Forensics Institute (NCFI). The NCFI provides a variety of basic cybercrime investigative courses for first responders and other personnel who do not already perform specialized cybercrime investigative functions.[152] The UCCTF illustrates some of the benefits of offsetting workload, which allows their cyber investigators to focus on criminal investigations by using digital forensic and cyber intelligence analysts to perform more technical investigative functions.[153] Providing basic training to and sharing cybercrime investigative responsibilities with personnel not assigned to the hybrid task forces presents opportunities to maximize the capabilities and capacity of the task forces members.

4. Threats

Like the conventional task forces and the internal resources models, agencies belonging to hybrid task forces depend on outside funding to maintain their cybercrime investigative capabilities and capacity. See Table 3. Agencies of all sizes that participate in this model often leverage federal grant funding and other reimbursement funds from the task forces fiduciary to acquire and maintain cybercrime investigative equipment and software licenses, as well as send personnel to specialized training.[154] This type of federal funding can be easily cut or diverted to other programs, and the current allocation of grant funding set aside for cyber enforcement efforts is inadequate for cybercrime enforcement needs.[155] The ongoing availability of outside funding sources, such as those from the federal government, is uncertain, and the drain on resources required to meet mandates from the funding source sometimes outweighs the benefits.[156] Recent data from a 2019 study showed how federal funding for cybercrime enforcement efforts was inadequate for the changing demands and the rapidly advancing nature of technology.[157] Most of the participating agencies in the hybrid

---

[152] National Computer Forensics Institute, "NCFI—Courses," National Computer Forensics Institute, accessed November 5, 2020, https://www.ncfi.usss.gov/ncfi/pages/courses.xhtml?dswid=1970.

[153] Police Executive Research Forum, *The Utah Model*, 5–6.

[154] Goodison, *Davis, and Jackson, Digital Evidence and the U.S. Criminal Justice System*, 16.

[155] Rhodes et al., Evaluation of the Multijurisdictional Task Forces, 70; Brandon Gaskew, *Reader's Guide to Understanding the U.S. Cyber Enforcement Architecture and Budget* (Washington, DC: Third Way, 2019), 13, https://thirdway.imgix.net/pdfs/override/Memo-Readers-Guide-Cyber-Budget.pdf.

[156] Dolliver, Collins, and Sams, "Hybrid Approaches to Digital Forensic Investigations," 131–33.

[157] Gaskew, *Reader's Guide to Understanding the U.S. Cyber*, 13.

task forces model lack enough internal funding to cover the ongoing costs of training, equipment, and other specialized cybercrime investigative resources if the federal funding was diverted or otherwise no longer available.[158] Agencies that participate in this type of model should have enough internal funding available to offset costs and ensure their ability to maintain their cybercrime investigative resources in the future.

Table 3. SWOT Analysis Matrix.

	STRENGTHS	WEAKNESSES	OPPORTUNITIES	THREATS
INTERNAL RESOURCES	Case prioritization dictated solely by the agency.	Workload capacity challenges.	Increasing cybercrime investigative capabilities throughout the agency by providing more training related to cybercrime investigative functions to patrol officers and other investigators.	Lack of funding for the initial and ongoing costs of having cybercrime capabilities and capacity.
CONVENTIONAL TASK FORCES	Consistent and ongoing specialized training and skills development opportunities for assigned personnel.	Lack of jurisdictional control over case prioritization.	Increasing the cybercrime investigative capabilities of agencies throughout the region by providing their personnel with more training related to cybercrime investigative functions.	Ongoing challenges with outside funding sources.
HYBRID TASK FORCES	Case prioritization is still primarily controlled by the home agency with the added benefits of the task forces model.	Decentralized makeup limits investigative coordination and hands-on training and expertise development for assigned personnel.	Increasing cybercrime investigative responsibilities of personnel not assigned to the task forces by providing training related to cybercrime investigative functions.	Ongoing challenges with outside funding sources.

[158] Goodison, Davis, and Jackson, *Digital Evidence and the U.S. Criminal Justice System*, 16–17.

D. CONCLUSION

When applied to the internal resources, conventional task forces, and hybrid task forces models described in this study, the SWOT analysis framework revealed commonalities and differences related to their impact on cybercrime investigative capabilities and capacity. The analysis was specific to attributes with the biggest impact on capabilities and capacity-level of cybercrime investigative training and expertise development for personnel, prioritization of cybercrime-related cases, and funding sources. Examining these attributes using the SWOT framework was useful in determining the impact of the different models on the cybercrime investigative capabilities and capacity of local law enforcement agencies.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. FINDINGS, RECOMMENDATIONS, AND CONCLUSION

This chapter discusses the main findings of this study and their implications for local law enforcement agencies and on future research. It summarizes findings for each of the three models and provides recommendations for agencies of varying sizes to consider regarding cybercrime investigative capabilities and capacity. The chapter concludes by answering the research question that formed the foundation for this thesis: of the three models identified in this study—internal resources, conventional task forces, and hybrid task forces—which one or combination thereof is best suited for agencies of different sizes?

A. FINDINGS OF THE ANALYSIS

The analysis of the three models revealed commonalities and differences between them that relate to agencies of different sizes. The findings also revealed that no matter what model an agency employs or participates in, they all have relative challenges. The results of the analysis are important to local law enforcement decision makers and much needed future research in this problem space.

1. Commonalities between the Models

The SWOT analysis of three models revealed commonalities between them. As illustrated in Chapter III, Table 3, the most prominent commonalities were in the opportunities and threats analysis sections.

a. Opportunities for Cybercrime Investigative Training

For opportunities, the analysis showed that providing more training to agency personnel who do not serve in cybercrime task forces or internal specialized cybercrime investigative roles would help increase the overall workload capacity for all three models. Ensuring patrol officers have adequate levels of basic cybercrime investigative training was a common theme in the research based on their integral role in the initial phases of the cybercrime investigative process. Data from a 2013 BJS LEMAS survey reinforced this commonality by revealing how trainee officers from a large cross-section of local and state law enforcement agencies throughout the nation only received three hours of cybercrime-

related training in the basic training academy.[159] Cybercrime training provides benefits ranging from being able to recognize cases that require additional work by cybercrime investigative specialists, to helping reduce the backlog cases.[160] The information presented in this study clearly showed a need for more cybercrime investigative involvement from first responders and other personnel not serving in cybercrime investigative roles, as cited in the Opportunities section of the analysis for all three models.

b. Threats Related to Funding

All three models shared similar threats related to funding. The cost of having resources in the form of specially trained personnel and specialized tools was cited in the study as a significant expense for individual agencies and task forces alike. The research for this study cited a lack of adequate funding as an ongoing challenge for all three models. The research also revealed how all three models, to some degree, depended on outside funding, such as from the federal government. Studies, such as those cited from PERF in 2014 and the Third Way in 2019, supported the funding challenges described in the Threats section of the analysis for all three models and provided data revealing the ongoing threat to internal and external funding sources.[161] Decreased funding for cybercrime enforcement efforts in California was also cited as a challenge.[162] Due to the reliance on government funding, challenges associated with the cost of building and maintaining cybercrime investigative capabilities will likely continue into the future.

c. Strengths Related to Case Prioritization

The internal resources and hybrid task forces models shared similarities associated with case prioritization. The research cited in the Strengths section of the analysis for the internal resources and hybrid task forces models listed how having flexibility for case

---

159 Reaves, *State and Local Law Enforcement Training Academies, 2013*, 7.

160 Goodison, Davis, and Jackson, Digital Evidence and the U.S. Criminal Justice System, 17; Wexler, *New National Commitment Required*, 59–63.

161 Gaskew, *Reader's Guide to Understanding the U.S. Cyber*, 13; Wexler, *The Role of Local Law Enforcement*, 7.

162 High Technology Crime Advisory Committee, *High Technology Crime in California*, 7.

prioritization was not only a benefit of participation in both models but important for local law enforcement agencies. The importance of agencies having the ability to prioritize cases based on jurisdictional needs was highlighted by the research cited throughout the study. A cited case study in the Strengths section of the analysis for the internal resources model highlighted how a large agency used its ability to prioritize cybercrime investigative actions in a high-profile investigation that resulted in timely arrests and subsequent criminal prosecution for multiple suspects.[163] Although the internal resources model differed slightly from the hybrid task forces model by allowing for a greater level of autonomy to prioritize cases, the hybrid task forces model allowed for a similar level of case prioritization as described in the case study cited previously.

2. Differences between the Models

As illustrated in Chapter III, Table 3, prominent differences occurred between the three models revealed in the weakness' category.

a. Weaknesses Related to Workload with Internal Resources

Although the research revealed workload challenges as a common thread with all the cybercrime investigative efforts, the internal resources model described in this study was impacted the most based on increasing demands for cybercrime investigative support coupled with a lack of available expertise. The research revealed how most local law enforcement agencies did not have enough personnel to keep up with the volume of cybercrime investigative needs, which was a reason for participating in multijurisdictional task forces models. Data specific only to the internal resources described in this study was provided in the Weaknesses section of the analysis showing cybercrime investigative workload increases with two large police agencies in Australia and one in the United States.[164] The study showed that internal resources were more prone to capacity-related challenges than conventional and hybrid task forces.

---

[163] Wexler, *New National Commitment Required*, 35–36.

[164] Harkin, Whelan, and Chang, "The Challenges Facing Specialist Police Cyber-Crime Units," 524.

b. Weaknesses Related to Case Prioritization with Conventional Task Forces

The analysis exposed how the conventional task forces model when compared to the internal resources and hybrid task forces models did not allow participating agencies the same level of control over prioritizing cases. The research for this study cited how personnel assigned to conventional task forces were beholden to task forces case priorities and requests for investigative support from their home agencies were sometimes delayed. Data listed in the Weaknesses section of the analysis for the conventional task forces model revealed a disproportionately low number of cases being investigated by conventional task forces representing multiple agencies in large regions of California.[165] The study provides areas of concern for the level of prioritization cases received from all the agencies that participate in a conventional task forces model.

c. Weaknesses Related to Decentralization with Hybrid Task Forces

The analysis highlighted how the decentralized nature of hybrid task forces models described in this study was a weakness when compared to the conventional task forces model. As listed in the Weaknesses section of the analysis for the hybrid task forces models, investigative coordination, ongoing training, and other on-the-job skills development opportunities were more inhibited in the hybrid models when compared to the collocation of personnel with different skill levels common with conventional task forces. The research cited in this study provided evidence for the weaknesses of the hybrid task forces models as described.

B. RECOMMENDATIONS

The following recommendations were formulated based on the findings of this study. They are intended to assist decision makers from local law enforcement agencies

---

[165] High Technology Crime Advisory Committee, *High Technology Crime in California*, 5; National White Collar Crime Center, *California IC3 2010 Internet Crime Report*, 1; Indianapolis Metropolitan Police Department, *IDMP Quarterly Report:First Quarter 2019*, 11; Indianapolis Metropolitan Police Department, *IDMP Quarterly Report: Second Quarter 2019*, 12; Indianapolis Metropolitan Police Department, *IDMP Quarterly Report: Third Quarter 2019*, 12; Indianapolis Metropolitan Police Department, *IDMP Quarterly Report: Fourth Quarter 2019*, 12; Indianapolis Metropolitan Police Department, *IDMP 2017 Annual Report*, 66.

when developing policies for addressing cybercrime investigative capabilities and capacity. The recommendations are grouped by their relevance to different size agencies. As defined in this study, small agencies have fewer than 60 officers or serve populations of fewer than 60,000, midsize agencies have between 60 and 99 officers or serve populations between 60,000 to 99,000, and large agencies have over 99 officers or serve populations over 99,000. As was noted in this study, the size of an agency was an important consideration when developing policies related to the agency's cybercrime investigative capabilities and capacity.

1. Small and Midsize Local Law Enforcement Agencies

Based on the findings from this study, a recommendation for both small and midsize agencies to consider regarding their cybercrime investigative capabilities and capacity is participation in the hybrid task forces models and limited consolidation.

a. Participate in Hybrid Task Forces Models

As listed in the Commonalities between the Models section of the analysis findings, the hybrid models described in this study allow for small and midsize agencies with less resources to have access to free training and specialized equipment while offering flexibility with personnel deployment and case prioritization that thus combine the strengths described in the analysis of both the internal and conventional task forces models. Of the hybrid models described in this study, ECTF was particularly well suited for small and midsize agencies by providing the most flexibility with personnel commitment and case prioritization. Three of the eight small and midsize agencies that responded to our survey participated in the ECTF and all cited the free training and equipment as important benefits.

b. Consolidate and Share Internal Cybercrime Resources

Another recommendation for small and midsize agencies to consider is shared internal cybercrime investigative resources through limited consolidation or regionalized efforts between a small number of jurisdictions in the same area. As listed in the Differences between the Models section of the analysis findings, a weakness of the hybrid

task forces models was their decentralized nature. Limited consolidation may provide for the fusion of strengths from all three models as highlighted in the Analysis Findings section. As described in the findings, a weakness of conventional task forces models, as compared to strengths of the internal resources and hybrid models was less control over case prioritization. Smaller scale regionalization associated with the limited consolidation described previously is more likely to mitigate some of the case prioritization challenges associated with large regional conventional task forces as described in this study. This type of limited regionalization is conducive to the UCCTF hybrid task forces model as described in this study but is also compatible with the ECTF hybrid task forces model. This recommendation is best suited for small and midsize agencies that have existing mutual aid agreements or established cooperative relationships.

2. Large Local Law Enforcement Agencies

Based on the findings from this study, a recommendation for large agencies to consider regarding their cybercrime investigative capabilities and capacity is having their own internal resources combined with participation in the hybrid or conventional task forces models.

a. Combine Internal Resources with Hybrid or Conventional Task Forces Models

The research cited provided confirmation that the jurisdictional needs of large local law enforcement agencies combined with the benefits of participation in regionalized efforts creates an argument for them having internal resources and for participating in multijurisdictional cybercrime task forces models.[166] As listed in the Commonalities between the Models section of the analysis findings, the common strengths of the internal and hybrid task forces models would benefit large agencies that need to be able to prioritize cases to control the workload. Furthermore, the different weaknesses of the three models described in the differences between the Models section of the analysis findings are likely

[166] Nowacki and Willits, "An Organizational Approach to Understanding Police Response," 71; Wexler, *The Role of Local Law Enforcement*, 23.

to be offset by the common strengths described in the Commonalities between the Models section of the analysis findings.

3. Small, Midsize, and Large Local Law Enforcement Agencies

Based on the findings from this study, a recommendation for all small, midsize, and large agencies to consider regarding their cybercrime investigative capabilities and capacity is to increase the capabilities and capacity of personnel who do not serve in cybercrime investigative roles throughout the agency.

a. Train to Increase Cybercrime Capabilities for All Agency Personnel

The practice of housing all an agency's personnel with cybercrime investigative knowhow into a single unit not only reduces the workload capacity of the cybercrime investigative specialists, but fails to account for the connection of cybercrimes with other traditional crimes.[167] As listed in the Commonalities between the Models section of the analysis findings, the research cited in the shared opportunities between the models established a common argument for providing patrol officers and other personnel basic and ongoing cybercrime training.

C. CONCLUSION

In answering the research question that established the foundation for this thesis, of three common models local law enforcement agencies employ to address cybercrime investigative capabilities and capacity (internal resources, conventional task forces, and hybrid task forces models), is one or a combination thereof adaptable enough for small, midsize, and large agencies?

A clear argument can be made for hybrid task forces models being the most adaptable for achieving some level of cybercrime capabilities and capacity; however, it is not a "one size fits all" solution.

---

[167] Wexler, *New National Commitment Required*, 70–71.

As the findings of this study clearly showed, arguments can be made for each of the models depending on jurisdictional-specific variables of the agencies that employ them. It is for these reasons that combinations of the models were cited in the recommendations for small and midsize, as well as large local law enforcement agencies.

To continue to serve and protect their communities effectively, local law enforcement agencies must have the ability to address the gamut of ways cybercriminals are leveraging technology to victimize people today and into the future. Small, midsize, and large agencies are still finding it difficult to overcome challenges associated with funding and rigid, non-flexible organizational models that continue to compromise their cybercrime capabilities and capacity. Local law enforcement decision makers are currently grappling and will continue to grapple with making informed policy decisions related to their agencies' cybercrime investigative capabilities and capacity.

This study clearly highlighted the need for more research to expand the body of work related to the different models available for local law enforcement. Despite the prevalence of cybercrime, little in the way of this type of research is related to the current strategies local law enforcement agencies are employing to address the need for cybercrime investigative capabilities and capacity. Future research into the effectiveness of each model that includes more quantitative and qualitative data is recommended. A means for local law enforcement decision makers would be provided to make more informed decisions about which model would work best for their specific jurisdictional needs.

The effective distribution of cybercrime investigative knowhow throughout local law enforcement agencies and especially among first responders is recommended for future research. It was clear from the research for this study that local law enforcement agencies need to have personnel trained in how to identify cybercrimes and perform basic investigative functions regardless of whether the agency has its own internal cybercrimes unit or participates in one of the task forces models. As indicated in this study, it is important not only to control the workload of cybercrime investigative specialists, but also for increasing the agency's overall cybercrime investigative capacity. Subsequent research should focus on what level of cybercrime investigative training should be provided to both new and experienced officers, as well as those serving in special assignments. Additionally,

an emphasis should be placed on some level of standardized cybercrime curriculum for law enforcement agencies throughout the nation.

The research for this thesis attempted to determine how three common models local law enforcement agencies employ for addressing cybercrime investigative capabilities and capacity are at serving their intended purpose. This thesis adds to the body of knowledge about the strategies being used by local law enforcement agencies to increase their ability to address the growing problem of cyber-related crimes.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. LOCAL LAW ENFORCEMENT AGENCY QUESTIONNAIRE

A. SURVEYS

For the purpose of this questionnaire, cybercrime investigative resources refers to personnel with the training and skills to conduct digital forensics and investigations of crimes that occur in cyberspace or that are associated with the use of computers/digital devices. This document is part of a thesis research project related to local law enforcement's ability to conduct cybercrime investigations. The information collected may be used as qualitative data in the project. The responses can be anonymized so that the respondent and specific agency are not named.

Agency: _____Total Sworn & Civilian Personnel Employees: _____
Can your agency be named in the study? Yes / No

1. Does the agency have internal cybercrime investigative resources or are they outsourced?

2. Does the agency have a dedicated cybercrime unit or other specialized unit the focuses on digital crimes? How many sworn and nonsworn employees are assigned full-time, part-time, as a collateral assignment, or combination thereof?

3. If the agency does not have a dedicated cybercrimes or other specialized digital crimes unit, are there specialty trained sworn or nonsworn personnel who perform cybercrime-related functions?

4. Explain the level of cybercrime training patrol officers, detectives, and cybercrime specialists receive.

Please send responses or questions associated with this thesis project to:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

5. Explain how having a dedicated cybercrime unit or internal cybercrime specialization has benefitted the organization.

6. Does your agency belong to a multijurisdictional cybercrime taskforce (TF) or other formal or informal multijurisdictional partnership?

7. Explain how the partnership works.

8. Explain the benefits of belonging to the TF for the agency.

Please send responses or questions associated with this thesis project to:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

For the purpose of this questionnaire, cybercrime investigative resources refers to personnel with the training and skills to conduct digital forensics and investigations of crimes that occur in cyberspace or that are associated with the use of computers/digital devices. This document is part of a thesis research project related to local law enforcement's ability to conduct cybercrime investigations. The information collected may be used as qualitative data in the project. The responses can be anonymized so that the respondent and specific taskforce are not named.

Name of Taskforce:_____**Taskforce Type: Federal State Local**
Anonymized: Yes/ No

1. What is the total sworn and civilian personnel complement and how many local law enforcement agencies belong to the taskforce (TF)?

2. In what capacity do civilian staff serve?

3. Explain how the TF is set-up (centralized-TF members working out of a single location, decentralized- TF members working together from separate remote locations, or a combination thereof).

4. Explain how personnel are assigned to the TF (i.e. full-time, part-time, or combination thereof).

5. Explain how the TF affects the cybercrime investigative capabilities and capacity of participating agencies (i.e. available resources to engage cybercrime investigative activities and to manage labor-intensive aspects of cybercrime investigations).

For questions or concerns regarding this questionnaire or associated thesis project, contact:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

6. Explain the expectation or desired level of internal cybercrime investigative capabilities and capacity of agencies that belong to the TF.

7. Explain what involvement non-law enforcement entities have in the TF (e.g. private-sector and academia).

8. Explain the process for prioritizing investigations and any considerations for cases that originate from agencies that participate in the TF and those that do not.

For questions or concerns regarding this questionnaire or associated thesis project, contact:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

B. RESPONSES

1. Large Agencies

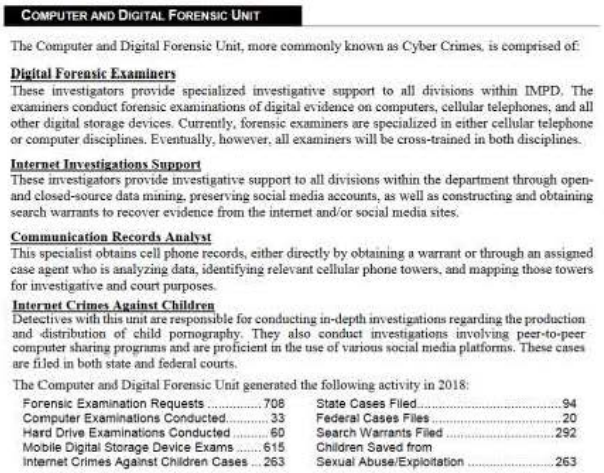
For the purpose of this questionnaire, cybercrime investigative resources refers to personnel with the training and skills to conduct digital forensics and investigations of crimes that occur in cyberspace or that are associated with the use of computers/digital devices. This document is part of a thesis research project related to local law enforcement's ability to conduct cybercrime investigations. The information collected may be used as qualitative data in the project. The responses can be anonymized so that the respondent and specific agency are not named.

Agency: Indianapolis Metropolitan Police Dept. (IMPD)
Total Sworn & Civilian Personnel Employees: approx. 2000
Can your agency be named in the study? Yes, provided an open source citation is used. The data can be found on pages 71 and 72 of IMPD 2018 Annual Report (see screenshots below).

1. Does the agency have internal cybercrime investigative resources or are they outsourced? *Internal.*

2. Does the agency have a dedicated cybercrime unit or other specialized unit the focuses on digital crimes? *IMPD has a full-time Computer and Digital Forensic Unit (CDFU).*

   How many sworn and nonsworn employees are assigned full-time, part-time, as a collateral assignment, or combination thereof? *IMPD has 13 full-time sworn investigators assigned to the CDFU. They perform a variety of duties:*



COMPUTER AND DIGITAL FORENSIC UNIT

The Computer and Digital Forensic Unit, more commonly known as Cyber Crimes, is comprised of:

Digital Forensic Examiners
These investigators provide specialized investigative support to all divisions within IMPD. The examiners conduct forensic examinations of digital evidence on computers, cellular telephones, and all other digital storage devices. Currently, forensic examiners are specialized in either cellular telephone or computer disciplines. Eventually, however, all examiners will be cross-trained in both disciplines.

Internet Investigations Support
These investigators provide investigative support to all divisions within the department through open- and closed-source data mining, preserving social media accounts, as well as constructing and obtaining search warrants to recover evidence from the internet and/or social media sites.

Communication Records Analyst
This specialist obtains cell phone records, either directly by obtaining a warrant or through an assigned case agent who is analyzing data, identifying relevant cellular phone towers, and mapping those towers for investigative and court purposes.

Internet Crimes Against Children
Detectives with this unit are responsible for conducting in-depth investigations regarding the production and distribution of child pornography. They also conduct investigations involving peer-to-peer computer sharing programs and are proficient in the use of various social media platforms. These cases are filed in both state and federal courts.

The Computer and Digital Forensic Unit generated the following activity in 2018:

Forensic Examination Requests	708	State Cases Filed	94
Computer Examinations Conducted	33	Federal Cases Files	20
Hard Drive Examinations Conducted	60	Search Warrants Filed	292
Mobile Digital Storage Device Exams	615	Children Saved from Sexual Abuse/Exploitation	263
Internet Crimes Against Children Cases	263		

Please send responses or questions associated with this thesis project to:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

3. If the agency does not have a dedicated cybercrimes or other specialized digital crimes unit, are there specialty trained sworn or nonsworn personnel who perform cybercrime-related functions? *N/A*

4. Explain the level of cybercrime training patrol officers, detectives, and cybercrime specialists receive. *Investigators attend digital investigations training/certification. Levels of training vary from basic certifications and advanced training to Master's Degree in forensic computing and cybercrime investigations.*

5. Explain how having a dedicated cybercrime unit or internal cybercrime specialization has benefitted the organization.

   Benefits range from regular requests for examination of digital devices to inter-agency task force investigations. Most commonly, devices are seized daily on a routine basis during a variety of investigative circumstances. Search warrants on devices are very common now, and the dedicated forensic investigators are a key part of state and federal investigations. Prosecutors regularly ask for review of any seized devices for evidentiary value, and jurors now often expect these steps to be taken.

6. Does your agency belong to a multijurisdictional cybercrime taskforce (TF) or other formal or informal multijurisdictional partnership?

   Yes – Internet Crimes Against Children (ICAC) in partnership with FBI.

7. Explain how the partnership works.

   Investigators are credentialed through the FBI for child pornography/exploitation related investigations.

8. Explain the benefits of belonging to the TF for the agency.

   Participation provides FBI support and resources, including some overtime reimbursement for overtime expenses. Investigators gain experience and expertise testifying in state and federal court on cases with defenseless juvenile victims. The inter-agency relationship between IMPD and federal partners also provides important long-term benefits in working complex, sensitive cases.

Please send responses or questions associated with this thesis project to:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

For the purpose of this questionnaire, cybercrime investigative resources refer to personnel with the training and skills to conduct digital forensics and investigations of crimes that occur in cyberspace or that are associated with the use of computers/digital devices. This document is part of a thesis research project related to local law enforcement's ability to conduct cybercrime investigations. The information collected may be used as qualitative data in the project. The responses can be anonymized so that the respondent and specific agency are not named.

Agency: XXXXX
Total Sworn: 1235
Civilian Personnel Employees: 304

Can your agency be named in the study? No

1. Does the agency have internal cybercrime investigative resources or are they outsourced?

   We have a computer forensic unit comprised of 4 non-sworn computer forensic examiners.

   We also have a Child Predator Unit comprised of 2 sworn investigators.

2. Does the agency have a dedicated cybercrime unit or other specialized unit the focuses on digital crimes? How many sworn and nonsworn employees are assigned full-time, part-time, as a collateral assignment, or combination thereof?

   We do NOT have a dedicated cybercrimes unit. Investigators in several units around the department work cyber-crimes.

3. If the agency does not have a dedicated cybercrimes or other specialized digital crimes unit, are there specialty trained sworn or nonsworn personnel who perform cybercrime-related functions?

   See response to question number 1.

4. Explain the level of cybercrime training patrol officers, detectives, and cybercrime specialists receive.

   Computer Forensic Examiners are all IACIS certified. They are also CCLO and CCPA certified.

Please send responses or questions associated with this thesis project to:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

5. Explain how having a dedicated cybercrime unit or internal cybercrime specialization has benefitted the organization.

   Computers are used in an ever-increasing number of crimes. Having our own Computer Forensic Unit is a great benefit to our investigative units in obtaining digital evidence.

6. Does your agency belong to a multijurisdictional cybercrime taskforce (TF) or other formal or informal multijurisdictional partnership?

   Our Child Predator investigators are also task force officers with the FBI, HSI and the OSBI.

7. Explain how the partnership works.

   Our investigators work out of our office but join efforts with the other agencies when beneficial to the investigation.

8. Explain the benefits of belonging to the TF for the agency.

   This is of value when the crimes cross jurisdictional boundaries. It can also be helpful in filing federal charges when appropriate.

Please send responses or questions associated with this thesis project to:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

For the purpose of this questionnaire, cybercrime investigative resources refers to personnel with the training and skills to conduct digital forensics and investigations of crimes that occur in cyberspace or that are associated with the use of computers/digital devices. This document is part of a thesis research project related to local law enforcement's ability to conduct cybercrime investigations. The information collected may be used as qualitative data in the project. The responses can be anonymized so that the respondent and specific agency are not named.

Agency:_Santa Clara County Sheriff's Office
Sworn & Civilian Personnel Compliment: Sworn
Anonymized: No

1. Does the agency have internal cybercrime investigative resources or are they outsourced?

   We have our own internal Forensics unit, however we are partnered with multiple local and federal agencies which include: Federal -USSS and USMS Local – SJPD (Silicon Valley ICAC) and Santa Clara County DA's Office (Crime Lab)

2. Does the agency have a dedicated internal cybercrime/ digital crimes or other specialized cybercrime unit or other dedicated fulltime or part-time resources?

   We have our own Internal Cyber Crime Unit, as well as Units that are partnered with other Agencies. Our SAFE Task Force is internal, and focuses on primarily Sex Offender and Child Pornography / Exploitation cases. Our REACT Task Force is a combination of State, Federal and District Attorneys is a multi-agency task force and High Technology theft (IP Theft), BitCoin/Ransomware cases etc.

3. Explain the level of cybercrime training patrol officers, detectives, and cybercrime specialists receive.

   5 years ago, it was nonexistent. However with how advanced electronic devices such as phones and tablets have become, Patrol as well as the Investigation Bureau have realized the importance of understanding how they work to better assist their cases. Now- Patrol gets on average 16 hours a year of formal training, and about 24 hours of non-formal (through contacting Detectives such as myself who assist them in the field.) Investigation gets on average 40 hours a year on training, and those who specialize in the field / work closely where electronics play a part in the crime, receive up to 100+ hours a year on supplemental training.

4. Explain how having internal cybercrime capabilities has benefited the organization.

Basically, it has allowed Law Enforcement access into the Criminals diary (cell phone). With Google/Apple making such advances in their technology, we can literally track them via Google or Apple Maps, plot where they were, decipher their call logs etc. It's been huge as far as Law Enforcement goes.

5. Does your agency belong to a multijurisdictional cybercrime taskforce (TF) or other formal or informal multijurisdictional partnership?

   Yes, REACT, ICAC, and the USMS 290 Fugitive Task Force.

6. Explain how the partnership works.

   Essentially, we pick up caseloads pertaining to our designated areas, and either work the case up from the ground up, or assist with areas where help is needed. In the latter, the USMS for example need our help in Localizing warrants for California, and we need their help in Fugitive Apprehension for out of State cases. With the USSS, we rely on them for the latest training and they often provide us equipment our department can't afford. It also opens up the whole network of Detectives/Forensic Experts who we can call on when we run into issues. The benefits of being involved in a task force are HUGE.

7. Explain the benefits of belonging to the TF or other multijurisdictional partnership.

   Similar to the answer above, belonging to a TF allow us access to resources (both equipment and personnel) that we would have never had access to before. This means we are able to tackle the cases we wouldn't have been able to before without their help.

2. Midsize Agencies

For the purpose of this questionnaire, cybercrime investigative resources refers to personnel with the training and skills to conduct digital forensics and investigations of crimes that occur in cyberspace or that are associated with the use of computers/digital devices. This document is part of a thesis research project related to local law enforcement's ability to conduct cybercrime investigations. The information collected may be used as qualitative data in the project. The responses can be anonymized so that the respondent and specific agency are not named.

Agency: XXXXX **Total Sworn & Civilian Personnel Employees:** __181__ ___

Can your agency be named in the study? Yes / No

1. Does the agency have internal cybercrime investigative resources or are they outsourced?
   Outsourced (RCFL)

2. Does the agency have a dedicated cybercrime unit or other specialized unit the focuses on digital crimes? How many sworn and nonsworn employees are assigned full-time, part-time, as a collateral assignment, or combination thereof?
   No, Zero

3. If the agency does not have a dedicated cybercrimes or other specialized digital crimes unit, are there specialty trained sworn or nonsworn personnel who perform cybercrime-related functions?
   No

4. Explain the level of cybercrime training patrol officers, detectives, and cybercrime specialists receive.
   Minimal, mandated online yearly training (2 hour)

5. Explain how having a dedicated cybercrime unit or internal cybercrime specialization has benefitted the organization.
   N/A

6. Does your agency belong to a multijurisdictional cybercrime taskforce (TF) or other formal or informal multijurisdictional partnership?
   There is one (CATCH) but we don't have any personnel participating. We did several years ago and hope to again if we get to full staffing.

7. Explain how the partnership works.
   Their website has a very quick and concise description. https://catchteam.org/
   Regional agencies can participate if they wish to and supply/assign an officer.

Please send responses or questions associated with this thesis project to:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

8. Explain the benefits of belonging to the TF for the agency.

When we did participate, it provided us with an expedited response to any crimes requiring computer equipment examination and additional expertise via the officer assigned to the task force.

Please send responses or questions associated with this thesis project to:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

For the purpose of this questionnaire, cybercrime investigative resources refers to personnel with the training and skills to conduct digital forensics and investigations of crimes that occur in cyberspace or that are associated with the use of computers/digital devices. This document is part of a thesis research project related to local law enforcement's ability to conduct cybercrime investigations. The information collected may be used as qualitative data in the project. The responses can be anonymized so that the respondent and specific agency are not named.

Agency:___Mountain View Police Department_____**Sworn & Civilian**
Personnel Compliment:__97 Sworn _____
Anonymized: Yes/ No

1. Does the agency have internal cybercrime investigative resources or are they outsourced? Internal

2. Does the agency have a dedicated internal cybercrime/ digital crimes or other specialized cybercrime unit or other dedicated fulltime or part-time resources? Dedicated internal cyber-crimes investigations and digital forensic examinations.

3. Explain the level of cybercrime training patrol officers, detectives, and cybercrime specialists receive. For investigators/examiners joining the unit, we have designated the following list of training resources as essential:

   Prerequisite Training: (most of these course are free through NW3C)

CI 099 - Basic Computer Skills for Law Enforcement (BCS-WB)
CI 100 - Identifying and Seizing Electronic Evidence - Web Based (ISEE-WB)
CI 103 - Introduction to Cell Phone Investigations (ICPI-WB)
CI 141 - Encryption (ENC-WB)
CI 151 - First Responders & Digital Evidence (LC1-WB)
CI 152 - Search Warrants & Digital Evidence (LC2-WB)
CI 120 - Cell Phone Seizure and Acquisition (Formerly CPI) (CPSA)
CC 101 - Basic Data Forensic Imaging (BDFI) (Formerly BDRA)
CI 101- Secure Techniques for Onsite Previewing (STOP) ***Usually offered same week as BDFI
CC 201 - Intermediate Data Recovery and Analysis (IDRA)
CC 215 - Macintosh® Triage and Imaging (MTI)
CC 225 - Apple® iDevice Forensics (iDF)
CC 250 - Linux Open Source Forensics (LOSF)
CC 315 - Windows Artifacts (WinArt)
CC 320 - Windows Internet Trace Evidence (INET)
CC 325 - Macintosh® Forensic Analysis (MFA)

   Specialized training after assignment to the unit:

Cellebrite Logical and Physical
Black Bag technologies
XRY Examiner Level 2

XRY Examiner Level 3
OS Triage,
Magnet Axiom, and Forensic Explorer certifications
Autopsy Digital Forensics

4. Explain how having internal cybercrime capabilities has benefited the organization. Our forensic examiners are able to interface much easier and more effectively with the primary investigators regarding the digital evidence. We also have more control over the management of the backlog of examinations and are able to prioritize examinations based on investigative needs.

5. Does your agency belong to a multijurisdictional cybercrime taskforce (TF) or other formal or informal multijurisdictional partnership? Yes. We belong to the Internet Crimes Against Children (ICAC) task force, and the Electronic Crimes Task Force (ECTF.)

6. Explain how the partnership works. With ICAC we are assigned cases involving possessing and distribution of child pornography (assigned from NCMEC) that are believed to have occurred in our jurisdiction. Through or relationship with ICAC our agency receives training, equipment, and software licenses for forensic tools. This helps offset the cost of running the digital forensic lab in our department.

   With ECTF we are provided resources for training and equipment for digital forensics.

7. Explain the benefits of belonging to the TF or other multijurisdictional partnership. As indicated above we receive training, equipment, and software licenses used in our digital forensic examinations which helps offset the costs of maintaining the digital forensic lab.

For the purpose of this questionnaire, cybercrime investigative resources refers to personnel with the training and skills to conduct digital forensics and investigations of crimes that occur in cyberspace or that are associated with the use of computers/digital devices. This document is part of a thesis research project related to local law enforcement's ability to conduct cybercrime investigations. The information collected may be used as qualitative data in the project. The responses can be anonymized so that the respondent and specific agency are not named.

Agency: XXXXX **Total Sworn & Civilian Personnel Employees:** __156_- 92 officers

Can your agency be named in the study? No

1. Does the agency have internal cybercrime investigative resources or are they outsourced?

   We have internal cybercrime investigative resources.

2. Does the agency have a dedicated cybercrime unit or other specialized unit the focuses on digital crimes? How many sworn and nonsworn employees are assigned full-time, part-time, as a collateral assignment, or combination thereof?

   No, we do not have a dedicated unit that focuses on digital crimes. We have one sworn employee who does cybercrime investigations as a collateral assignment (he is a patrol officer who had been assigned to SVRCFL until this shift year, when we had to pull him back because patrol was short-staffed – now he does cyber on OT or adjusted time when necessary for big cases).

3. If the agency does not have a dedicated cybercrimes or other specialized digital crimes unit, are there specialty trained sworn or nonsworn personnel who perform cybercrime-related functions?

   Yes, see answer to #2 above.

4. Explain the level of cybercrime training patrol officers, detectives, and cybercrime specialists receive.

   Rudimentary high-level training occasionally provided at in-service training classes only.

Please send responses or questions associated with this thesis project to:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

5. Explain how having a dedicated cybercrime unit or internal cybercrime specialization has benefitted the organization.

   We're able to use our in-house expert (see answer to #2) on major cases as necessary; due to his relationship with the SVRCFL, he is allowed to use their resources on an individual case-by-case basis. If we didn't have this as an option, we'd be waiting longer to get evidence returns from the SVRCFL or another cybercrime TF.

6. Does your agency belong to a multijurisdictional cybercrime taskforce (TF) or other formal or informal multijurisdictional partnership?

   Until July 2018, we had a detective assigned to the SVRCFL for about 10 to 12 straight years. In July 2018, we had to pull the detective back to backfill for patrol staffing. As soon as our patrol staffing levels permit, we intend to send a detective back. It's a great resource.

7. Explain how the partnership works.

   When we had a detective assigned to the SVRCFL, they worked there full-time in a five-year maximum assignment.

8. Explain the benefits of belonging to the TF for the agency.

   They were able to prioritize cases for our agency, and the TF would expend additional resources to assist a member agency. Our evidence got turned around faster than it otherwise would, which helped us to prosecute cases more efficiently.

Please send responses or questions associated with this thesis project to:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

For the purpose of this questionnaire, cybercrime investigative resources refers to personnel with the training and skills to conduct digital forensics and investigations of crimes that occur in cyberspace or that are associated with the use of computers/digital devices. This document is part of a thesis research project related to local law enforcement's ability to conduct cybercrime investigations. The information collected may be used as qualitative data in the project. The responses can be anonymized so that the respondent and specific agency are not named.

Agency: _____RCPD_____**Total Sworn & Civilian Personnel Employees:** _140-ish___96 sworn

Can your agency be named in the study? Yes / No

1. Does the agency have internal cybercrime investigative resources or are they outsourced? Both

2. Does the agency have a dedicated cybercrime unit or other specialized unit the focuses on digital crimes? How many sworn and nonsworn employees are assigned full-time, part-time, as a collateral assignment, or combination thereof? No.

3. If the agency does not have a dedicated cybercrimes or other specialized digital crimes unit, are there specialty trained sworn or nonsworn personnel who perform cybercrime-related functions? Yes

4. Explain the level of cybercrime training patrol officers, detectives, and cybercrime specialists receive. Various specialized training courses for cell phone forensics & tracking, dark web investigations, crypto currency, and social media investigations.

Please send responses or questions associated with this thesis project to:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

5. Explain how having a dedicated cybercrime unit or internal cybercrime specialization has benefitted the organization.

   Allows for a more thorough and efficient investigation of cyber related crimes.

6. Does your agency belong to a multijurisdictional cybercrime taskforce (TF) or other formal or informal multijurisdictional partnership?

   No.

7. Explain how the partnership works.

   N/A

8. Explain the benefits of belonging to the TF for the agency.

   N/A

Please send responses or questions associated with this thesis project to:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

3. Small Agencies

LOCAL LAW ENFORCMENT AGENCY QUESTIONAIRE 1

For the purpose of this questionnaire, cybercrime investigative resources refers to personnel with the training and skills to conduct digital forensics and investigations of crimes that occur in cyberspace or that are associated with the use of computers/digital devices. This document is part of a thesis research project related to local law enforcement's ability to conduct cybercrime investigations. The information collected may be used as qualitative data in the project. The responses can be anonymized so that the respondent and specific agency are not named.

Agency: BELMONT PD **Total Sworn & Civilian Personnel Employees:** 40

Can your agency be named in the study? Yes / No

1. Does the agency have internal cybercrime investigative resources or are they outsourced? INTERNAL
2. Does the agency have a dedicated cybercrime unit or other specialized unit the focuses on digital crimes? How many sworn and nonsworn employees are assigned full-time, part-time, as a collateral assignment, or combination thereof? ASSIGNED TO A DETECTIVE AS NEEDED.
3. If the agency does not have a dedicated cybercrimes or other specialized digital crimes unit, are there specialty trained sworn or nonsworn personnel who perform cybercrime-related functions? THEY ARE NOT TRAINED SPECIFICALLY IN CYBERCRIME.
4. Explain the level of cybercrime training patrol officers, detectives, and cybercrime specialists receive. MINIMAL, VIA PAST INVESTIGATIVE EXPERIENCE.

Please send responses or questions associated with this thesis project to:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

5. **Explain how having a dedicated cybercrime unit or internal cybercrime specialization has benefitted the organization.** N/A - WE DON'T HAVE ONE. COULD BE BENEFICIAL W/ SOME FRAUD CASES.

6. **Does your agency belong to a multijurisdictional cybercrime taskforce (TF) or other formal or informal multijurisdictional partnership?** NO WE ARE NOT.

7. **Explain how the partnership works.**

N/A

8. **Explain the benefits of belonging to the TF for the agency.**

N/A.

Please send responses or questions associated with this thesis project to:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

For the purpose of this questionnaire, cybercrime investigative resources refers to personnel with the training and skills to conduct digital forensics and investigations of crimes that occur in cyberspace or that are associated with the use of computers/digital devices. This document is part of a thesis research project related to local law enforcement's ability to conduct cybercrime investigations. The information collected may be used as qualitative data in the project. The responses can be anonymized so that the respondent and specific agency are not named.

Agency: East Palo Alto PD_____Total Sworn & Civilian Personnel Employees: __36.5
Can your agency be named in the study? Yes / No

1. Does the agency have internal cybercrime investigative resources or are they outsourced? Outsource

2. Does the agency have a dedicated cybercrime unit or other specialized unit the focuses on digital crimes? How many sworn and nonsworn employees are assigned full-time, part-time, as a collateral assignment, or combination thereof? No

3. If the agency does not have a dedicated cybercrimes or other specialized digital crimes unit, are there specialty trained sworn or nonsworn personnel who perform cybercrime-related functions? No

4. Explain the level of cybercrime training patrol officers, detectives, and cybercrime specialists receive. None

Please send responses or questions associated with this thesis project to:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

5. Explain how having a dedicated cybercrime unit or internal cybercrime specialization has benefitted the organization.

   N/A

6. Does your agency belong to a multijurisdictional cybercrime taskforce (TF) or other formal or informal multijurisdictional partnership?

   ICAC

7. Explain how the partnership works.

   ICAC manages all the cases

8. Explain the benefits of belonging to the TF for the agency.

   Availability of resources and experts

Please send responses or questions associated with this thesis project to:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

For the purpose of this questionnaire, cybercrime investigative resources refers to personnel with the training and skills to conduct digital forensics and investigations of crimes that occur in cyberspace or that are associated with the use of computers/digital devices. This document is part of a thesis research project related to local law enforcement's ability to conduct cybercrime investigations. The information collected may be used as qualitative data in the project. The responses can be anonymized so that the respondent and specific agency are not named.

Agency: Hillsborough PD **Total Sworn & Civilian Personnel Employees:** __37____

Can your agency be named in the study? Yes

1. Does the agency have internal cybercrime investigative resources or are they outsourced?
   Internal…Via specialist or Inspectors.

2. Does the agency have a dedicated cybercrime unit or other specialized unit the focuses on digital crimes? How many sworn and nonsworn employees are assigned full-time, part-time, as a collateral assignment, or combination thereof?

   Our Inspectors are trained and investigate cybercrimes. We also have a specialist that assists in complex cases. We do not have a dedicated unit.

3. If the agency does not have a dedicated cybercrimes or other specialized digital crimes unit, are there specialty trained sworn or nonsworn personnel who perform cybercrime-related functions?

   YES

4. Explain the level of cybercrime training patrol officers, detectives, and cybercrime specialists receive.

   Our Inspectors and specialist have been to relevant trainings. We also have a state-of the art electronic forensics station, as well as mobile phone forensic hardware and software. Our specialist conducts forensic examinations for numerous outside agencies and was recognized by the San Mateo County DA's office for his outstanding work on a number of complex cases.

Please send responses or questions associated with this thesis project to:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

5. Explain how having a dedicated cybercrime unit or internal cybercrime specialization has benefitted the organization.

   We have solved cases through electronic forensics that would not have been solved in any other way. We solved an assault with a deadly weapon case through a cell phone forensic examination and a "SNAP-CHAT" warrant as an example.

6. Does your agency belong to a multijurisdictional cybercrime taskforce (TF) or other formal or informal multijurisdictional partnership?

   YES – Our specialist is a member of The United States Secret Service – San Francisco Electronic Crimes Task Force
   SFO-ECTF

7. Explain how the partnership works.

   We are eligible to be reimbursed for overtime on investigations and can put in requests for reimbursement on equipment expenses relating to cybercrime.

8. Explain the benefits of belonging to the TF for the agency.

   The sharing of knowledge and resources. The ability to procure equipment. Unique training opportunities

Please send responses or questions associated with this thesis project to:
Ryan Monaghan
Lieutenant
San Mateo Police Department
Naval Postgraduate School Center for Homeland Defense & Security
ryan.monaghan@nps.edu

For the purpose of this questionnaire, cybercrime investigative resources refers to personnel with the training and skills to conduct digital forensics and investigations of crimes that occur in cyberspace or that are associated with the use of computers/digital devices. This document is part of a thesis research project related to local law enforcement's ability to conduct cybercrime investigations. The information collected may be used as qualitative data in the project. The responses can be anonymized so that the respondent and specific agency are not named.

Agency:__Monterey County DA Office____**Sworn & Civilian Personnel Compliment:**__Yes_
Anonymized: Yes/ No

1. Does the agency have internal cybercrime investigative resources or are they outsourced?
    a. We utilize both. Internally we have 3 sworn and 1 non-sworn Investigators with working knowledge of various digital forensic aspects. However, if a situation arises where we don't have the necessary tools, we will outsource the evidence.

2. Does the agency have a dedicated internal cybercrime/ digital crimes or other specialized cybercrime unit or other dedicated fulltime or part-time resources?
    a. Within our Digital Forensic lab, we have 1 non-sworn Investigator whose full time job is to work on digital forensic cases. The 3 sworn Investigators work in the lab on a lateral assignment basis, meaning they still carry a full workload outside of working on digital forensic cases.

3. Explain the level of cybercrime training patrol officers, detectives, and cybercrime specialists receive.
    a. They have attended various courses offered by California Department of Justice, National White Collar Crime Center, National Computer Forensic Institute, San Jose ICAC. As well as have attended tool specific training such as Cellebrite, EnCase and BlackBag Technologies. All four Investigators assigned to the lab have been working in Digital Forensics for over 8 years.

4. Explain how having internal cybercrime capabilities has benefited the organization.
    a. Since we receive cases from all police agencies within the county, having the ability to do the examinations in- house has been a great benefit. When attorneys bring in a witness for an interview, having the capabilities to download a phone, pull surveillance footage, etc. at a moments notice has produced invaluable evidence for various cases.
    b. We are able to prioritize the incoming cases based on the needs of the office rather than first come first serve.

5. Does your agency belong to a multijurisdictional cybercrime taskforce (TF) or other formal or informal multijurisdictional partnership?
    a. Yes, we belong to a cybercrime taskforce with the Secret Service and San Jose ICAC

6. Explain how the partnership works.
    a. In regards to both taskforces, they send us to training and give us equipment at no cost to the agency.
    b. The taskforces also have been very helpful with locating resources when we come across a case that we do not have the proper software or tools to complete.
    c. In return, the Monterey County District Attorney's Office provides assistance whenever needed and statistics showing all digital forensics completed.

7. Explain the benefits of belonging to the TF or other multijurisdictional partnership.
    a. A couple of the benefits of belonging to a taskforce are the following:
        i. Collaboration with other investigators all over the United States
        ii. Ability to attend training and receive certifications
        iii. Receiving equipment that our agency otherwise might not have been able to afford
        iv. Continued education and learning how other agencies work, allowing our agency to adapt and grow

LIST OF REFERENCES

Bandl, Steven G. “The Characteristics and Structure of Police Organizations.” In *Police in America*, ch. 3. Thousand Oaks, CA: SAGE Publications, Inc., 2018.

Becerra, Xavier. “High Technology Theft Apprehension and Prosecution (HTTAP) Program.” State of California Department of Justice, Office of the Attorney General, December 13, 2011. https://oag.ca.gov/ecrime/httap.

Bednar, Peter, Vasilios Katos, and Cheryl Hennell. “The Complexity of Collaborative Cyber Crime Investigations.” *Digital Evidence and Electronic Signature Law Review* 6 (2009): 214–219. https://doi.org/10.14296/deeslr.v6i0.1894.

Breslin, Michael. “The U.S. Secret Service Electronic Crimes Task Forces: Employing Public-Private Sector Partnerships to Combat Cybercrime.” *Police Chief*, July 2017. https://www.policechiefmagazine.org/wp-content/uploads/PoliceChief_July2017_F-web.pdf.

Bureau of Justice Assistance. *The Utah Model: A Path Forward for Investigating and Building Resilience to Cyber Crime*. Washington, DC: Bureau of Justice Assistance, 2017. http://www.iacpcybercenter.org/wp-content/uploads/2015/04/The-Utah-Model-A-Path-Forward-for-Investigating-and-Building-Resilience-to-Cybercrime.pdf.

Callagy, Michael P. “Can Local Police and Sheriff’s Departments Provide a Higher Degree of Homeland Security Coordination and Collaboration through Consolidation of Police Services?” Master’s thesis, Naval Postgraduate School, 2010. https://calhoun.nps.edu/bitstream/handle/10945/5123/10Sep_Callagy.pdf?sequence=1&isAllowed=y.

CATCH. “CATCH: Computer and Technology Crimes High Tech Task Force.” Accessed May 18, 2019. https://catchteam.org/.

Commonwealth of Australia. *National Plan to Combat Cybercrime*. ACT, Australia: Commonwealth of Australia, 2013. https://sherloc.unodc.org/res/cld/lessons-learned/aus/national-plan-to-combat-cybercrime_html/National_Plan_to_Combat_Cybercrime.pdf.

Department of Homeland Security. *2017 National Network of Fusion Centers Final Report*. Washington, DC: Department of Homeland Security, 2017. https://www.dhs.gov/sites/default/files/publications/2017_National_Network_of_Fusion_Centers_Final%20Report.pdf.

———. *U.S. Department of Homeland Security Cybersecurity Strategy*. Washington, DC: Department of Homeland Security, 2018. https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

———. *United State Secret Service Electronic Crimes Task Force*. Washington, DC: Department of Homeland Security, 2014. https://www.dhs.gov/sites/default/files/publications/USSS_Electronic-Crimes-TaskForces.pdf.

Dolliver, Diana S., Carson Collins, and Beau Sams. "Hybrid Approaches to Digital Forensic Investigations: A Comparative Analysis in an Institutional Context." *Digital Investigation* 23 (December 2017): 124–137. https://doi.org/10.1016/j.diin.2017.10.005.

Eoyang, Mieke, Allison Peters, Ishan Mehta, and Brandon Gaskew. *To Catch A Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors*. Washington, DC: Third Way, 2018. https://thirdway.imgix.net/pdfs/override/To_Catch_A_Hacker_Report.pdf.

Finklea, Kristin, and Catherine A. Theohary. *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*. CRS Report No. R42547. Washington, DC: Congressional Research Service, 2015. https://www.hsdl.org/?view&did=762027.

Flory, Teri A. "Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies." Master's thesis, Purdue University, 2015. https://docs.lib.purdue.edu/open_access_theses/1220.

Gaskew, Brandon. *Reader's Guide to Understanding the U.S. Cyber Enforcement Architecture and Budget*. Washington, DC: Third Way, 2019. https://thirdway.imgix.net/pdfs/override/Memo-Readers-Guide-Cyber-Budget.pdf.

Gavin, Brady. "What Is A SIM Card (And What Comes Next)?." *How-to Geek*. Accessed July 22, 2020. https://www.howtogeek.com/353634/what-is-a-sim-card/.

Global Advisory Committee. *Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers*. Washington, DC: Global Advisory Committee, 2015. https://it.ojp.gov/GIST/178/File/Cyber%20Integration%20for%20Fusion%20Centers.pdf/.

Gogolin, Greg, and James Jones. "Law Enforcement's Ability to Deal with Digital Crime and the Implications for Business." *Information Security Journal: A Global Perspective* 19, no. 3 (2010): 109–117. https://doi.org/10.1080/19393555.2010.483931.

Goodison, Sean E., Robert C. Davis, and Brian A. Jackson. *Digital Evidence and the U.S. Criminal Justice System*. Santa Monica, CA: RAND, 2015. https://www.rand.org/pubs/research_reports/RR890.html.

Harkin, Diarmaid, Chad Whelan, and Lennon Chang. “The Challenges Facing Specialist Police Cyber-Crime Units: An Empirical Analysis.” *Police Practice and Research* 19, no. 6 (November 2018): 519–536. https://doi.org/10.1080/15614263.2018.1507889.

Harmon, Rachel A. “Federal Programs and the Real Costs of Policing.” *New York University Law Review* 90, no. 3 (June 2015): 870–960.

Helms, Marilyn M., and Judy Nixon. “Exploring SWOT Analysis—Where Are We Now? A Review of Academic Research from the Last Decade.” *Journal of Strategy and Management* 3, no. 3 (2010): 215–251. https://doi.org/10.1108/17554251011064837.

Hendrickson, David. *High Technology Theft Apprehension & Prosecution Program Progress Report*. San Jose, CA: Santa Clara County District Attorney’s Office, 2010. https://info.publicintelligence.net/REACTOct-Dec09.pdf.

High Technology Crime Advisory Committee. *High Technology Crime in California—FY09/10*. Mather, CA: California Emergency Management Agency, 2010. https://oag.ca.gov/sites/all/files/agweb/pdfs/ecrime/2010_httap_report.pdf.

Hinduja, Sameer. “Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future.” *International Journal of Cyber Criminology* 1, no. 1 (2007): 1–26. https://doi.org/10.5281/zenodo.18275.

———. “Perceptions of Local and State Law Enforcement Concerning the Role of Computer Crime Investigative Teams.” *Policing: An International Journal* 27, no. 3 (September 2004): 341–357. https://doi.org/10.1108/13639510410553103.

Holt, Thomas J., and Adam M. Bossler. “Predictors of Patrol Officer Interest in Cybercrime Training and Investigation in Selected United States Police Departments.” *Cyberpsychology, Behavior, and Social Networking* 15, no. 9 (December 2012): 464–472. https://doi.org/10.1089/cyber.2011.0625.

Hyland, Shelley S., and Elizabeth Davis. *Local Police Departments, 2016: Personnel*. NCJ 252835. Washington, DC: Bureau of Justice Statistics, 2019. www.bjs.gov/content/pub/pdf/lpd16p.pdf.

Internet Crimes Complaint Center. *2017 Internet Crime Report*. Washington, DC: Federal Bureau of Investigation, 2017. https://pdf.ic3.gov/2017_IC3Report.pdf.

———. *2018 Internet Crime Report*. Washington, DC: Federal Bureau of Investigation, 2018. https://pdf.ic3.gov/2018_IC3Report.pdf.

Jefferis, Eric S., James Frank, Brad W. Smith, Kenneth J. Novak, and Lawrence F. Travis, III. “An Examination of the Productivity and Perceived Effectiveness of Drug Task Forces.” *Police Quarterly* 1, no. 3 (September 1998): 85–107. https://doi.org/10.1177/109861119800100306.

Langworthy, Robert H. “Lemas: A Comparative Organizational Research Platform.” *Justice Research and Policy* 4, no. 1–2 (December 1, 2002): 21–38. https://doi.org/10.3818/JRP.4.1.2002.21.

Marcum, Catherine D., and George E. Higgins. “Combating Child Exploitation Online: Predictors of Successful ICAC Task Forces.” *Policing: A Journal of Policy and Practice* 5, no. 4 (2011): 310–316. https://doi.org/10.1093/police/par044.

Marcum, Catherine D., George E. Higgins, Tina L. Freiburger, and Melissa L. Ricketts. “Policing Possession of Child Pornography Online: Investigating the Training and Resources Dedicated to the Investigation of Cyber Crime.” *International Journal of Police Science & Management* 12, no. 4 (2010): 516–525. https://doi.org/10.1350%2Fijps.2010.12.4.201.

Montgomery County Maryland Operating Budget. “Montgomery County Maryland Operating Budget: Police.” Accessed September 30, 2019. https://apps.montgomerycountymd.gov/BASISOPERATING/Common/Department.aspx?ID=47D.

National Archive of Criminal Justice Data. “Law Enforcement Management and Administrative Statistics (LEMAS) Series.” Accessed November 19, 2019. https://www.icpsr.umich.edu/icpsrweb/NACJD/series/92.

National Computer Forensics Institute. “NCFI—Courses.” National Computer Forensics Institute. Accessed November 5, 2020. https://www.ncfi.usss.gov/ncfi/pages/courses.xhtml?dswid=1970.

National White Collar Crime Center. *California IC3 2010 Internet Crime Report*. Glen Allen, VA: National White Collar Crime Center, 2011. https://www.ic3.gov/media/annualreport/2010/California%202010%20Report.pdf.

Northern California Computer Crimes Task Force. “About NC3TF.” Accessed May 18, 2019. https://www.nc3tf.org/about.

Nowacki, Jeffrey, and Dale Willits. “An Organizational Approach to Understanding Police Response to Cybercrime.” *Policing: An International Journal* 43, no. 1 (November 2019): 63–76. https://doi.org/10.1108/PIJPSM-07-2019-0117.

Pfeifer, Joseph W., and Ophelia Roman. “Tiered Response Pyramid: A System-Wide Approach to Build Response Capability and Surge Capacity.” *Homeland Security Affairs* 12, art. 5 (December 2016). https://www.hsaj.org/articles/13324.

Pickton, David W., and Sheila Wright. “What’s SWOT in Strategic Analysis?.” *Strategic Change* 7, no. 2 (1998): 101–109. https://doi.org/10.1002/(SICI)1099-1697(199803/04)7:2%3C101::AID-JSC332%3E3.0.CO;2-6.

Police Executive Research Forum. *The Utah Model: A Path Forward for Investigating and Building Resilience to Cyber Crime*. Washington, DC: Bureau of Justice Assistance, 2017. http://www.iacpcybercenter.org/wp-content/uploads/2015/04/The-Utah-Model-A-Path-Forward-for-Investigating-and-Building-Resilience-to-Cybercrime.pdf.

Povero, David. “Municipal Police Agencies Dial 911 When It Comes to Investigating Cyber-Related Crimes in the Future?.” *Journal of California Law Enforcement* 49, no. 3 (2015): 14–19. ProQuest.

REACT—Regional Enforcement Allied Computer Team. “About Us.” Accessed February 25, 2019. http://www.reacttf.org/reacttf/d/index.html?#/page/about.

Reaves, Brian A. *Local Police Departments, 2013: Personnel, Policies, and Practices*. NCJ 248677. Washington, DC: Bureau of Justice Statistics, 2015. https://www.bjs.gov/content/pub/pdf/lpd13ppp.pdf.

———. *State and Local Law Enforcement Training Academies, 2013*. NCJ 249784. Washington, DC: Bureau of Justice Statistics, 2013. https://www.bjs.gov/content/pub/pdf/slleta13.pdf.

Rhodes, William, Christina Dyous, Meg, Chapman, Michael Shively, Dana Hunt, and Kristen Wheeler. *Evaluation of the Multijurisdictional Task Forces (MJTFs), Phase II: MJTF Performance Monitoring Guide*. NCJ 228942. Cambridge, MA: Abt Associates Inc., 2009. https://www.ncjrs.gov/pdffiles1/nij/grants/228942.pdf.

Shipley Todd G., and Art Bowker. “Introduction to Internet Crime.” In *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, edited by Nick Selby, 1–20. Waltham, MA: Elsevier Science & Technology Books, 2013. ProQuest.

Smith, Brad W., Kenneth J. Novak, James Frank, and Lawrence F. Travis III. “Multijurisdictional Drug Task Forces: An Analysis of Impacts.” *Journal of Criminal Justice* 28, no. 6 (November–December 2000): 543–556. https://doi.org/10.1016/S0047-2352(00)00069-6.

Stambaugh, Hollis, David S. Beaupre, David J. Icove, Richard Baker, Wayne Cassaday, and Wayne P. Williams. *Electronic Crime Needs Assessment for State and Local Law Enforcement*. NCJ 186276. Washington, DC: Department of Justice, Office of Justice Programs, 2001.

Stock, Stephen, Michael Bott, Mark Villarreal, and Luke Johnson. “Hackers Steal Millions from Bay Area Residents by Targeting Cellphones in ‘SIM Swap’ Scams.” NBC Bay Area, May 23, 2019. https://www.nbcbayarea.com/news/local/hackers-steal-millions-from-bay-area-residents-by-targeting-cell-phones-in-sim-swap-scams/189712/.

Symantec Corporation. *2017 Norton Cyber Security Insights Report Global Results*. Mountain View, CA: Symantec Corporation, 2017. https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf.

United States Government Accountability Office. *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*. GAO-07-705. Washington, DC: United States, 2007. https://www.gao.gov/new.items/d07705.pdf.

Wexler, Chuck. *New National Commitment Required: The Changing Nature of Crime and Criminal Investigations*. Washington, DC: Police Executive Research Forum, 2018.

———. *The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime*. Washington, DC: Police Executive Research Forum, 2014. https://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf.

Willits, Dale, and Jeffrey Nowacki. “The Use of Specialized Cybercrime Policing Units: An Organizational Analysis.” *Criminal Justice Studies* 29, no. 2 (June 2016): 1–42. https://doi.org/10.1080/1478601X.2016.1170282.

Yesilyurt, Hamdi. “The Response of American Police Agencies to Digital Evidence.” PhD diss., University of Central Florida, 2011. https://stars.library.ucf.edu/etd/1732.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California